日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ９月２９日

出 願 番 号
Application Number: 平成１１年特許願第２７７２６５号

出 願 人
Applicant (s): 株式会社日立製作所

T. Fujiyama et al
filed 7-27-00
703-684-1120
TSM-13

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ５月１２日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０３３８３０

HT 150901

【書類名】　特許願

【整理番号】　HL12573000

【提出日】　平成11年 9月29日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 9/06

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　藤山　達也

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　萱島　信

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　永井　康彦

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報システム事業部内

【氏名】　角田　光弘

【発明者】

【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　情報システム事業部内

【氏名】　山田　知明

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100087170

【弁理士】

【氏名又は名称】　富田　和子

【手数料の表示】

【予納台帳番号】　012014

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】セキュリティ評価方法および装置、セキュリティ施策の作成支援方法および装置

【特許請求の範囲】

【請求項１】

電子計算機を用いて、１以上の機器で構成されるシステムに施されたセキュリティを評価するセキュリティ評価方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定を受け付ける第１のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第１のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された評価対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第２のステップと、

前記第１のステップで指定された評価対象システムを構成する機器毎に、前記第２のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示し、前記入力装置を介して、操作者より、当該機器毎に対応付けて表示されたセキュリティ施策の実施の有無を受け付ける第３のステップと、

前記第３のステップで受け付けた評価対象システムを構成する各機器のセキュリティ施策の実施の有無に基づいて、当該評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を前記表示装置に表示する第４のステップと、を有すること

を特徴とするセキュリティ評価方法。

【請求項２】

請求項１記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が対応付けられて記述されており、

前記第４のステップは、前記第２のステップで読み出した評価対象システムを構成する各機器のセキュリティ施策を、当該セキュリティ施策に対応付けられたセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されたセキュリティ施策の数に対する前記第３のステップで実施有りとされたセキュリティ施策の数の割合を求め、これを当該種類に対するセキュリティ施策の達成度として、セキュリティの種類各々の達成度を前記表示装置に表示すること

を特徴とするセキュリティ評価方法。

【請求項３】

請求項１記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリティ施策を施すことにって回避される危険度とが併せて記述されており、

前記第４のステップは、前記第２のステップで読み出した評価対象システムを構成する各機器のセキュリティ施策を、当該セキュリティ施策に対応付けられたセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第３のステップで実施無しとされたセキュリティ施策に対応付けられた危険度の総和を求め、これを当該種類に対するセキュリティ施策の残存危険度として、セキュリティの種類各々の残存危険度を前記表示装置に表示すること

を特徴とするセキュリティ評価方法。

【請求項４】

請求項１記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリティ施策を施すのにかかるコストとが併せて記述されており、

前記第４のステップは、前記第２のステップで読み出した評価対象システムを構成する各機器のセキュリティ施策を、当該セキュリティ施策に対応付けられたセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第３のステップで実施有りとされたセキュリテ

ィ施策に対応付けられたコストの総和を求め、これを当該種類に対するセキュリティ施策の所要コストとして、セキュリティの種類各々の所要コストを前記表示装置に表示すること

を特徴とするセキュリティ評価方法。

【請求項５】

請求項１記載のセキュリティ評価方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティのレベルが併せて記述されており、

前記第１のステップは、前記入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定に加えて、当該システムに施すべきセキュリティ施策のレベルの指定を受け付け、

前記第２のステップは、前記データベースから、前記第１のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策であって、前記第１のステップで指定されたレベル以下のセキュリティ施策を読み出すこと

を特徴とするセキュリティ評価方法。

【請求項６】

請求項１、２、３、４または５記載のセキュリティ評価方法であって、

前記第１のステップは、

前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか１つの指定を評価対象システムの指定として受け付けるステップと、

評価対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々の評価対象システムでの使用の有無を、評価対象システムを構成する各機器の指定として受け付けるステップと、を有すること

を特徴とするセキュリティ評価方法。

【請求項７】

電子計算機に、１以上の機器で構成されるシステムに施されたセキュリティを評価させるためのプログラムが記憶された記憶媒体であって、

前記プログラムは、前記電子計算機に、

当該電子計算機に接続された入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定を受け付ける第１のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第１のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された評価対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第２のステップと、

前記第１のステップで指定された評価対象システムを構成する機器毎に、前記第２のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示し、前記入力装置を介して、操作者より、当該機器毎に対応付けて表示されたセキュリティ施策の実施の有無を受け付ける第３のステップと、

前記第３のステップで受け付けた評価対象システムを構成する各機器のセキュリティ施策の実施の有無に基づいて、当該評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を前記表示装置に表示する第４のステップと、を実行させること

を特徴とするプログラムが記憶された記憶媒体。

【請求項８】

１以上の機器で構成されるシステムに施されたセキュリティを評価するセキュリティ評価装置であって、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースと、

前記データベースに記述されているシステムタイプをすべて読み出して表示し、操作者より、表示中のシステムタイプのうちのいずれか１つの指定を評価対象

システムの指定として受け付ける第１の指示受付手段と、

前記第１の指示受付手段にて評価対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して表示し、操作者より、表示中の構成機器各々の評価対象システムへの使用の有無を、評価対象システムを構成する各機器の指定として受け付ける第２の指示受付手段と、

前記第１の指示受付手段にて評価対象システムとして指定されたシステムタイプの構成機器のうち、前記第２の指示受付手段にて評価対象システムを構成する機器として指定された各構成機器に施すべきセキュリティ施策を、前記データベースから読み出して表示し、操作者より、表示中の各構成機器に施すべきセキュリティ施策の実施の有無を受け付ける第３の指示受付け手段と、

前記第３の指示受付け手段で受け付けた各構成機器のセキュリティ施策の実施の有無に基づいて、前記評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を表示する評価手段と、を有すること

を特徴とするセキュリティ評価装置。

【請求項９】

電子計算機を用いて、１以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援するセキュリティの構築支援方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定を受け付ける第１のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第１のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第２のステップと、

前記第１のステップで指定された支援対象システムを構成する機器毎に、前記第２のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示する第３のステップと、を有すること

を特徴とするセキュリティの構築支援方法。

【請求項１０】

請求項９記載のセキュリティの構築支援方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が対応付けられて記述されており、

前記第２のステップは、前記データベースから、前記第１のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策とその種類を読み出し、

前記第３のステップは、前記第１のステップで指定された支援対象システムを構成する機器毎に、前記第２のステップで読み出した支援対象システムを構成する各機器のセキュリティ施策とその種類を対応付けて、前記表示装置に表示すること

を特徴とするセキュリティの構築支援方法。

【請求項１１】

請求項９記載のセキュリティの構築支援方法であって、

前記データベースは、記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティのレベルが併せて記述されており、

前記第１のステップは、前記入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定に加えて、当該システムに施すべきセキュリティ施策のレベルの指定を受け付け、

前記第２のステップは、前記データベースから、前記第１のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策であって、前記第１のステップで指定されたレベル以下のセキュリティ施策を読み出すこと

を特徴とするセキュリティの構築支援方法。

【請求項１２】

請求項９、１０または１１記載のセキュリティの構築支援方法であって、

前記第１のステップは、

前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか１つの指定を支援対象システムの指定として受け付けるステップと、

支援対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々の支援対象システムでの使用の有無を、支援対象システムを構成する各機器の指定として受け付けるステップと、を有すること

を特徴とするセキュリティの構築支援方法。

【請求項１３】

電子計算機に、１以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援させるためのプログラムが記憶された記憶媒体であって、

前記プログラムは、前記電子計算機に、

前記電子計算機に接続された入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定を受け付ける第１のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第１のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第２のステップと、

前記第１のステップで指定された支援対象システムを構成する機器毎に、前記第２のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に表示する第３のステップと、を実行させること

を特徴とするプログラムが記憶された記憶媒体。

【請求項１４】

１以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援

するセキュリティの構築支援装置であって、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースと、

前記データベースに記述されているシステムタイプをすべて読み出して表示し、操作者より、表示中のシステムタイプのうちのいずれか１つの指定を支援対象システムの指定として受け付ける第１の指示受付手段と、

前記第１の指示受付手段にて支援対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して表示し、操作者より、表示中の構成機器各々の支援対象システムでの使用の有無を、支援対象システムを構成する各機器の指定として受け付ける第２の指示受付手段と、

前記第１の指示受付手段にて支援対象システムとして指定されたシステムタイプの構成機器のうち、前記第２の指示受付手段にて支援対象システムを構成する機器として指定された各構成機器に施すべきセキュリティ施策を、前記データベースから読み出し、機器毎に表示するセキュリティ施策表示手段と、を有すること

を特徴とするセキュリティの構築支援装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、１つ以上の機器で構成されるシステムに対し、当該システムに施されたセキュリティの状態を評価し、あるいは、当該システム固有のセキュリティ施策の作成を支援する技術に関する。

【０００２】

【従来の技術】

企業のビジネス活動において、インターネット技術に基づく情報システムが重要なインフラとなってきている。また、企業内情報システムのインターネット接続に対する関心が高まるにつれて、企業内情報システムに対する不正アクセスやウィルスによる情報資産の破壊などのセキュリティ問題が認知されるようになってきている。

【０００３】

このようなセキュリティ問題から情報システムを守るため、従来、企業は、個々のセキュリティ問題に対してファイアウォールの設置やウィルス対策ソフトの導入などの個別の技術的対策を行なっていた。しかし、近年では、情報システム全体に対する脅威を分析してセキュリティ状態を評価し、その評価結果に基づいて今後の対策方針を作成することにより、対象となる情報システム固有のセキュリティ対策を総合的に実施することが求められるようになりつつある。

【０００４】

このような背景から、情報技術製品やこれらの製品で構成された情報システムのセキュリティを体系的に評価・構築するための枠組みとして、セキュリティ評価基準ＣＣ（Common Criteria）が１９９９年６月に国際標準化された（IS 15408）。また、個々の情報システムに施すべきセキュリティポリシーの事例を提示したものとして、米国のセキュリティ専門家であるCharles Cresson Wood氏が作成した運用管理中心のセキュリティポリシー事例集ＩＳＰＭＥ（Information Security Policy Made Easy）が１９９７年６月１０日にBASELINE software社より出版された。

【０００５】

そして、コンサルタントサービスとして、上記のセキュリティ評価基準ＣＣやセキュリティポリシー事例集ＩＳＰＭＥに基づいて、情報システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援するサービスを提供する者が現れてきている。

【０００６】

【発明が解決しようとする課題】

ところで、上記のセキュリティ評価基準ＣＣに基づいて、情報システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援する場合、体系的に規定されたセキュリティ評価基準ＣＣから、セキュリティ状態の評価対象あるいはセキュリティ施策作成の支援対象となる情報システムを構成する各機器に適用されるべき基準を抽出し、当該情報システムに固有の基準を作成しなければならない。このため、セキュリティ評価基準ＣＣを熟知した、高度な専門知識を有す

るものでなければ実施することができない。したがって、実施に多くの時間がかかり、また、作業コストも高くなる。

【０００７】

また、上記のセキュリティポリシー事例集ＩＳＰＭＥに基づいて、セキュリティ施策の作成を支援する場合においても、当該事例集ＩＳＰＭＥのなかからセキュリティ施策作成の支援対象となる情報システムに対応する事例を抽出し、抽出した事例を、当該情報システムの実際の構成に当てはめながら当該情報システムに対するセキュリティポリシーを作成しなければならない。このため、やはり、セキュリティポリシー事例集ＩＳＰＭＥと情報システムの実際の構成の対応関係を熟知した、高度な専門知識を有するものでなければ実施することができない。したがって、実施に多くの時間がかかり、また、作業コストも高くなる。

【０００８】

本発明は、上記の事情に鑑みてなされたものであり、高度な専門的知識がなくても、システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援することを可能にすることを目的とする。

【０００９】

【課題を解決するための手段】

上記課題を解決するために、本発明の第１の態様は、電子計算機を用いて、１以上の機器で構成されるシステムに施されたセキュリティを評価するセキュリティ評価方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、評価対象システムと当該システムを構成する各機器の指定を受け付ける第１のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第１のステップで指定された評価対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された評価対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第２のステップと、

前記第１のステップで指定された評価対象システムを構成する機器毎に、前記第２のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に

接続された表示装置に表示し、前記入力装置を介して、操作者より、当該機器毎に対応付けて表示されたセキュリティ施策の実施の有無を、たとえばチェックリスト形式で受け付ける第３のステップと、

前記第３のステップで受け付けた評価対象システムを構成する各機器のセキュリティ施策の実施の有無に基づいて、当該評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を前記表示装置に表示する第４のステップと、を有することを特徴とする。

【００１０】

ここで、前記第１のステップは、たとえば、前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか１つの指定を評価対象システムの指定として受け付けるステップと、評価対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々の評価対象システムでの使用の有無を、評価対象システムを構成する各機器の指定として、たとえばチェックリスト形式で受け付けるステップと、からなるものであってもよい。

【００１１】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が併せて記述されている場合、前記第４のステップは、たとえば、評価対象システムを構成する各機器のセキュリティ施策をセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策の数に対する前記第３ステップで実施有りとされたセキュリティ施策の数の割合を求め、これを当該種類に対するセキュリティ施策の達成度として、セキュリティの種類各々の達成度を前記表示装置に表示するようにしてもよい。

【００１２】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリ

ティ施策を施すことにって回避される危険度（この危険度は、たとえば、そのセキュリティ施策を施さなかったことにより発生する可能性のある年間損害額として表わされる）とが併せて記述されている場合、前記第４のステップは、たとえば、評価対象システムを構成する各機器のセキュリティ施策をセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第３ステップで実施無しとされたセキュリティ施策の危険度の総和を求め、これを当該種類に対するセキュリティ施策の残存危険度として、セキュリティの種類各々の残存危険度を前記表示装置に表示するようにしてもよい。

【００１３】

あるいは、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類とそのセキュリティ施策を施すのにかかるコスト（このコストは、たとえば、そのセキュリティ施策を施すのにかかる年間コストとして表わされる）とが併せて記述されている場合、前記第４のステップは、たとえば、評価対象システムを構成する各機器のセキュリティ施策をセキュリティの種類毎に分類し、セキュリティの種類毎に、当該種類に分類されるセキュリティ施策のうち、前記第３ステップで実施有りとされたセキュリティ施策のコストの総和を求め、これを当該種類に対するセキュリティ施策の所要コストとして、セキュリティの種類各々の所要コストを前記表示装置に表示するようにしてもよい。

【００１４】

本態様では、操作者が、入力装置を用いて、評価対象システムとその構成機器を指定すると、当該評価対象システムを構成する機器毎に、その機器に施すべきセキュリティ施策のリストが表示装置に表示される。操作者は、表示装置に表示された各機器のセキュリティ施策を見て、入力装置を用いて、たとえば表示中のセキュリティ施策にチェックする（いわゆるチェックリスト形式）ことで、その実施の有無を入力することができる。操作者が、入力装置を用いて、表示装置に表示された各機器のセキュリティ施策の実施の有無を入力すると、それに基づいて、評価対象システムに施されたセキュリティ状態の評価を行ない、その結果を表示装置に表示する。

【００１５】

このように、本態様によれば、操作者が評価対象システムとその構成機器を指定するだけで、その構成機器各々に施すべきセキュリティ施策が表示される。そして、操作者が表示されている各構成機器のセキュリティ施策の実施の有無を入力するだけで、その評価対象システムに施されているセキュリティの評価を行なうことができる。したがって、操作者は、高度な専門的知識がなくても、システムのセキュリティ状態を評価することが可能となる。

【００１６】

次に、上記課題を解決するために、本発明の第２の態様は、電子計算機を用いて、１以上の機器で構成されるシステムに施すべきセキュリティ施策の作成を支援するセキュリティの構築支援方法であって、

前記電子計算機に接続された入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定を受け付ける第１のステップと、

システムタイプ毎に、構成機器と当該構成機器に施すべきセキュリティ施策とが記述されたデータベースを検索し、前記第１のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策を読み出す第２のステップと、

前記第１のステップで指定された支援対象システムを構成する機器毎に、前記第２のステップで読み出したセキュリティ施策を対応付けて、前記電子計算機に接続された表示装置に、たとえばリスト形式で表示する第３のステップと、を有することを特徴とする。

【００１７】

ここで、前記第１のステップは、たとえば、前記データベースに記述されているシステムタイプをすべて読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中のシステムタイプのうちのいずれか１つの指定を支援対象システムの指定として受け付けるステップと、支援対象システムとして指定されたシステムタイプの構成機器すべてを前記データベースから読み出して前記表示装置に表示し、前記入力装置を介して、操作者より、表示中の構成機器各々

の支援対象システムでの使用の有無を、支援対象システムを構成する各機器の指定として、たとえばチェックリスト形式で受け付けるステップと、からなるものであってもよい。

【００１８】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティの種類が併せて記述されている場合、前記第２のステップは、前記データベースから、前記第１のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策とその種類を読み出し、前記第３のステップは、前記第１のステップで指定された支援対象システムを構成する機器毎に、前記第２のステップで読み出した支援対象システムを構成する各機器のセキュリティ施策とその種類を対応付けて、前記表示装置に表示するようにしてもよい。

【００１９】

また、前記データベースに記述されているセキュリティ施策各々に、そのセキュリティ施策を施すことによって確保されるセキュリティのレベルが併せて記述されている場合、前記第１のステップは、前記入力装置を介して、操作者より、支援対象システムと当該システムを構成する各機器の指定に加えて、当該システムに施すべきセキュリティ施策のレベルの指定を受け付け、前記第２のステップは、前記データベースから、前記第１のステップで指定された支援対象システムに対応するシステムタイプの構成機器のうち、前記第１のステップで指定された支援対象システムを構成する各機器に施すべきセキュリティ施策であって、前記第１のステップで指定されたレベル以下のセキュリティ施策を読み出すようにしてもよい。

【００２０】

本態様では、操作者が、入力装置を用いて、支援対象システムとその構成機器を指定すると、当該支援対象システムを構成する機器毎に、その機器に施すべきセキュリティ施策のリストが表示装置に表示される。このように、本態様によれば、操作者が支援対象システムとその構成機器を指定するだけで、その構成機器

各々に施すべきセキュリティ施策が表示されるので、操作者は、高度な専門的知識がなくても、システムに施すべきセキュリティ施策を構築することが可能となる。

【００２１】

【発明の実施の形態】

以下に、本発明の実施の形態について説明する。

【００２２】

まず、本発明の第１実施形態について説明する。

【００２３】

図１は、本発明の第１実施形態が適用されたセキュリティ支援・評価装置１の概略構成図である。

【００２４】

図１に示すように、本実施形態のセキュリティ支援・評価装置１１は、ＣＰＵ１１と、メモリ１２と、ハードディスク装置などの外部記憶装置１３と、ＣＤ－ＲＯＭやＦＤなどの可搬性を有する記憶媒体１５からデータを読み取る読取り装置１４と、キーボードやマウスなどの入力装置１６と、ディスプレイなどの表示装置１７と、ネットワークに接続された通信装置１８と、上述した各構成要素間のデータ送受を司るインターフェース１９とを備えた、一般的な構成を有する電子計算機上に構築することができる。

【００２５】

ここで、外部記憶装置１３には、本実施形態のセキュリティ支援・評価装置１１を電子計算機上に構築するためのセキュリティ評価・構築支援プログラムＰＧ１３２が格納されており、ＣＰＵ１１がメモリ１２上にロードされたこのプログラム１３２を実行することにより、操作者が指定した対象システムの構成機器各々に施すべきセキュリティ施策のリストを作成する施策リスト生成部１１１と、操作者から受け付けた対象システムの構成機器各々に施すべきセキュリティ施策の実施の有無に基づいて、当該対象システムのセキュリティ状態を評価するセキュリティ評価部１１２と、入力装置１６や表示装置１７を制御して操作者から各種指示を受け付けたり、施策リスト生成部１１１やセキュリティ評価部１１２か

らの出力を表示する入出力制御部１１３とを、プロセスとして実現する。

【００２６】

なお、このプログラム１３２は、読取り装置１４によりＣＤ－ＲＯＭやＦＤなどの可搬性の記憶媒体１５から読み取られ、外部記憶装置１３にインストールされるようにしてもよいし、あるいは、通信装置１８によりネットワークから外部記憶装置１３にダウンロードされるようにしてもよい。また、図１では、このプログラム１３２を、一旦外部記憶装置１３に格納してから、メモリ１２上にロードしてＣＰＵ１１により実行するようにしているが、読取り装置１４により可搬性の記憶媒体１５から読み取って直接メモリ１２上にロードしＣＰＵ１１により実行するようにしてもよい。あるいは、通信装置１８を介してネットワークから直接メモリ１２上にロードしＣＰＵ１１により実行するようにしてもよい。

【００２７】

また、外部記憶装置１３には、本実施形態によるセキュリティ評価・構築支援の適用が予定されるシステムのタイプ毎に、システムの構成機器各々に適用すべきセキュリティ施策が記述された施策データベースDB_1～DB_n１３１が予め格納されている。本実施形態では、セキュリティ評価・構築支援の適用が予定されるシステムのタイプとして、インターネット接続システム、認証システムおよびプラントシステムを想定している。

【００２８】

図２～図５に、施策データベースの一例を示す。

【００２９】

ここで、図２および図３はインターネット接続システムに対応して設けられた施策データベースの内容を示しており、図４は認証システムに対応して設けられた施策データベースの内容を示している。そして、図５はプラントシステム対応して設けられた施策データベースの内容を示している。

【００３０】

図２～図５において、列２０１には、施策種別（セキュリティの種類）が記述される。列２０２には、同じ行の施策種別の欄に記述されたセキュリティを確保するためのセキュリティ施策が記述される。列２０３には、同じ行のセキュリテ

ィ施策の欄に記述されたセキュリティ施策が想定している想定脅威が記述される。列２０４には、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策について、セキュリティ評価基準ＣＣ（IS 15408）に規定されていれるセキュリティ機能要件（Security Functional Requirement）のカタログから、その施策を満たす機能要件を選択したものが記述される。列２０５_{i}には、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策について、それが所定業種（たとえば、金融業など）の基準において実施が義務づけられていればその旨記述される。

【００３１】

また、$列２０６_{i}$は、対象システムの構成機器として使用されることが予定される機器毎に設けられ、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策が適用可能である場合に、そのセキュリティ施策を適用することにより確保されるセキュリティのレベルＬ１～Ｌ３と、そのセキュリティ施策を適用するために必要とされる年間の所要コストＣ１～Ｃ５と、そのセキュリティ施策を適用しなかったことにより同じ行の想定脅威の欄に記述された想定脅威が現実のものとなった場合における年間の損害額を示した残存リスクＲ１～Ｒ５とが記述される。

【００３２】

また、列２０７は、対象システムの構成機器として使用されることが予定される各機器が設置される施設について、$列２０６_{i}$と同様に、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策が適用可能である場合に、そのセキュリティ施策を適用することにより確保されるセキュリティのレベルＬ１～Ｌ３と、そのセキュリティ施策を適用するために必要とされる年間の所要コストＣ１～Ｃ５と、そのセキュリティ施策を適用しなかったことにより同じ行の想定脅威の欄に記述された想定脅威が現実のものとなった場合における年間の損害額を示した残存リスクＲ１～Ｒ５とが記述される。

【００３３】

そして、列２０８は、対象システムの運用について、$列２０６_{i}$と同様に、同じ行のセキュリティ施策の欄に記述されたセキュリティ施策が適用可能である場

合に、そのセキュリティ施策を適用することにより確保されるセキュリティのレベルＬ１～Ｌ３と、そのセキュリティ施策を適用するために必要とされる年間の所要コストＣ１～Ｃ５と、そのセキュリティ施策を適用しなかったことにより同じ行の想定脅威の欄に記述された想定脅威が現実のものとなった場合における年間の損害額を示した残存リスクＲ１～Ｒ５が記述される。

【００３４】

なお、セキュリティのレベルＬ１～Ｌ３、年間の所要コストＣ１～Ｃ５および年間の残存リスクＲ１～Ｒ５の具体的な値は、図２～図５に示すとおりである。

【００３５】

たとえば、図２および図３に示すインターネット接続システムに対応して設けられた施策データベースにおいて、セキュリティ施策「個人単位でパスワードを設定」は、施策種別「アクセス権限の管理」に属し、そのセキュリティ施策が想定している想定脅威が「不正使用」であり、また、その施策を満たすセキュリティ機能が、セキュリティ評価基準ＣＣ（IS 15408）に規定される機能要件「ＦＭＴ＿ＭＳＡ．１」であることを示している。また、このセキュリティ施策「個人単位でパスワードを設定」は、インターネット接続システムの構成機器のうちＷＷＷサーバおよびクライアントに適用可能であることを示している。そして、そのセキュリティ施策をＷＷＷサーバに適用することにより確保されるセキュリティのレベルはＬ３（最強）であり、そのセキュリティ施策をＷＷＷサーバに適用するために必要とされる年間の所要コストはＣ２（１００万未満）であり、そのセキュリティ施策をＷＷＷサーバに適用しなかったことにより想定脅威「不正使用」が現実のものとなった場合における年間の損害額（残存リスク）はＲ２（１００万未満）であることを示している。また、そのセキュリティ施策をクライアントに適用することにより確保されるセキュリティのレベルはＬ３（最強）であり、そのセキュリティ施策をクライアントに適用するために必要とされる年間の所要コストはＣ２（１００万未満）であり、そのセキュリティ施策をクライアントに適用しなかったことにより想定脅威「不正使用」が現実のものとなった場合における年間の損害額（残存リスク）はＲ２（１００万未満）であることを示している。

【００３６】

なお、図２～図５に示すデータベースの列２０６$_i$、２０７および２０８の各欄に記入する内容は、事前に行なった脅威分析やリスク分析等の結果に基づいて決定されるようにすることが好ましい。

【００３７】

次に、上記構成のセキュリティ支援・評価装置１の動作について説明する。

【００３８】

図６および図７は、本発明の第１実施形態であるセキュリティ支援・評価装置１の動作を説明するためのフロー図である。

【００３９】

まず、施策リスト生成部１１１は、入出力制御部１１３を用いて、表示装置１７に、外部記憶装置１３に記憶されている施策データベースＤＢ$_1$～ＤＢ$_n$１３１の対象システムの名称のリストを含んだ、図８に示すような、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの名称を選択するためのＧＵＩ画面を表示する（ステップＳ１００１）。

【００４０】

図８に示すようなＧＵＩ画面を介して、操作者により、入力装置１６を使って、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの名称が選択（図８ではインターネット接続システムが選択された例を示している）されると（ステップＳ１００２）、施策リスト生成部１１１は、選択されたシステムの構成機器の名称を外部記憶装置１３に記憶されている施策データベースＤＢ$_1$～ＤＢ$_n$１３１から読み出す。そして、入出力制御部１１３を用いて、表示装置１７に、選択されたシステムの構成機器の名称のリストを含んだ、図９に示すような、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの構成機器の選択するためのＧＵＩ画面（図９ではインターネット接続システムを対象システムとした例を示している）を表示する（ステップＳ１００３）。

【００４１】

なお、図９において、項目「機器構成」８０１は、対応する施策データベース

DB_1～DB_n１３１から読み出された、ステップＳ１００２で選択されたシステムを構成する機器のなかから、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムに実際に使用されている機器を選択するためのものであり、操作者は入力装置１６を使って使用している機器の名称にチェックを入れられるようになっている。項目「環境」８０２は、対象システムの構成機器が設置される施設や当該対象システムの運用を、セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象に含めるか否かを設定するためのものであり、操作者は入力装置１６を使って含めたいものにチェックを入れられるようになっている。また、項目「セキュリティ強度」８０３は、セキュリティ施策の作成支援あるいはセキュリティ状態の評価を実施する上でのセキュリティのレベルを設定するためのものであり、操作者は入力装置１６を使って設定したいレベルにチェックを入れられるようになっている。ここで、レベル「並」は、対象システムに対し、必要最小限のキュリティを確保することを目的として、セキュリティ施策の作成支援あるいはセキュリティ状態の評価を実施する場合にチェックすべきレベルであり、図２～図５に示すレベルＬ１に相当する。レベル「最強」は、最大限のキュリティを確保することを目的として、セキュリティ施策の作成支援あるいはセキュリティ状態の評価を実施する場合にチェックすべきレベルであり、図２～図５に示すレベルＬ３に相当する。そして、レベル「強」は、レベル「並」とレベル「最強」の中間に位置するレベルであり、図２～図５に示すレベルＬ２に相当する。また、ボタン「施策構築支援」８０４は、本装置１にセキュリティ施策の作成支援を行なわせる場合に選択すべきボタンであり、ボタン「セキュリティ評価」８０５は、本装置１にセキュリティ評価を行なわせる場合に選択すべきボタンである。

【００４２】

さて、図９に示すようなＧＵＩ画面を介して、操作者により、入力装置１６を使って、必要な項目にチェックが入れられ、ボタン８０４、８０５のいずれかが選択されると（ステップＳ１００４）、施策リスト生成部１１１は、ステップＳ１００２で選択されたシステムに対応する対応する施策データベースDB_1～DB_n１３１から必要な情報を読み出し、項目「機器構成」８０１にてチェックさ

れた機器および項目「環境」８０２にてチェックされた環境毎に、セキュリティ施策リストを作成する（ステップＳ１００５）。

【００４３】

以下に、セキュリティ施策リストの作成処理について、図９に示す場合（項目「機器構成」８０１にてWWWサーバとクライアントがチェックされ、項目「環境」８０２にて運用がチェックされた場合）を例にとり説明する。

【００４４】

まず、図２および図３に示すインターネット接続システムのデータベースの「WWWサーバ」の列２０６_1の各行において、同じ行のセキュリティ施策が適用可能であり、かつ、当該セキュリティ施策を適用した場合に確保されるセキュリティレベルが、図８の項目「セキュリティ強度」でチェックされたレベル（ここでは「並」＝Ｌ１）以下のものが記述された行に着目する。そして、着目した各行について、「WWWサーバ」の列２０６_1に記述された内容と同じ行の列２０１～２０４、２０５_iに記述された内容とを読み出し、これらを基にWWWサーバに対するセキュリティ施策リストを作成する。以上の処理を、「クライアント」の列２０６_2および「運用」の列２０８のそれぞれに対しても、同様に実行することで、クライアントに対するセキュリティ施策リストと運用に対するセキュリティ施策リストを作成する。

【００４５】

次に、施策リスト生成部１１１は、図９に示すような画面において、項目「機器構成」８０１にてチェックされた機器および項目「環境」８０２にてチェックされた環境毎に、セキュリティ施策リストを作成したならば、ステップＳ１００４で選択されたボタンがボタン「構築支援」８０４であるか、あるいはボタン「セキュリティ評価」８０５であるかを判別する（ステップＳ１００６）。

【００４６】

選択されたボタンが「構築支援」８０４である場合、施策リスト生成部１１１は、入出力制御部１１３を介して、表示装置１７に、ステップＳ１００５で作成した、項目「機器構成」８０１にてチェックされた機器および項目「環境」８０２にてチェックされた環境毎のセキュリティ施策リストを表示して、セキュリテ

ィ施策の作成を支援する（ステップＳ１００７）。

【００４７】

図１０は、セキュリティ施策の作成支援のために表示されるセキュリティ施策リストの一例を示した図である。この例では、図９に示すチェック内容にしたがって、図２および図３に示すインターネット接続システムのデータベースから作成されたリストを示している。ここで、WWWサーバ、クライアントおよび運用各々のセキュリティ施策リストは、別々に表示されるようになっており、操作者は入力装置１６を使ってタグ９０１を選択することにより、所望のセキュリティ施策リストを表示することができる。なお、符号９０２、９０３は、現在表示中のセキュリティ施策リストをスクロールさせるためのボタンである。

【００４８】

一方、ステップＳ１００６にて、選択されたボタンが「セキュリティ評価」８０５である場合、セキュリティ評価部１１２は、入出力制御部１１３を介して、表示装置１７に、ステップＳ１００５で作成した、項目「機器構成」８０１にてチェックされた機器および項目「環境」８０２にてチェックされた環境毎のセキュリティ施策リストに含まれるセキュリティ施策各々の実施の有無を確認するためのＧＵＩ画面を表示する（ステップＳ１００８）。

【００４９】

図１１は、セキュリティ評価のために表示されるセキュリティ施策の実施の有無を確認するためのＧＵＩ画面の一例を示した図である。この例では、図９に示すチェック内容にしたがって、図２および図３に示すインターネット接続システムのデータベースから作成されたリストに基づいて、ＧＵＩ画面を作成した例を示している。ここで、図１１に示すＧＵＩ画面は、図１０に示す表示画面に、同じ行に記述されたセキュリティ施策の実施の有無をチェックするための入力欄でなる列９０４が設けられた構成となっている。なお、ボタン「リセット」９０６は、列９０６の各入力欄のチェック内容をリセットし、再度チェックし直すためのものである。

【００５０】

さて、図１１に示すようなＧＵＩ画面を介して、操作者により、入力装置１６

を使って、各セキュリティ施策の実施の有無がチェックが入れられ、ボタン「実行」９０５が選択されると（ステップＳ１００９）、セキュリティ評価部１１２は、入出力制御部１１３を介して、表示装置１７に、図１２に示すような、操作者より達成すべきセキュリティの目標レベルを受け付けるためのＧＵＩ画面を表示する（ステップＳ１０１０）。

【００５１】

図１２に示す例では、図１１に示すＧＵＩ画面に表示された機器および環境各々について、セキュリティの目標レベルを、施策種別毎のセキュリティ施策数に対する実施（対策）済のセキュリティ施策数の割合で設定するか（９１０）、施策種別毎の実施済のセキュリティ施策による所要コストの総額で設定するか（９１１）、あるいは、施策種別毎の未実施（未対策）のセキュリティ施策による残存リスクの総額で設定するか（９１２）を、選択することができるようになっている。ここで、セキュリティの目標レベルを施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合で設定する場合には、オプションとして特定業界（業界Ａ、Ｂ）における基準を適用するか否かを選択できるようになっており、特定業界における基準の適用が選択された場合は、セキュリティの目標レベルが、施策種別毎の当該基準で義務づけられたセキュリティ施策数に対する実施済の当該基準で義務づけられたセキュリティ施策数の割合として設定される。なお、図１２では、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として８０％以上が設定された例を示している。

【００５２】

さて、図１２に示すようなＧＵＩ画面を介して、操作者により、入力装置１６を使って、セキュリティの目標レベルが設定されると（ステップＳ１０１１）、その設定内容にしたがって対象システムのセキュリティ状態を評価する（ステップＳ１０１２）。

【００５３】

たとえば、ステップＳ１０１１において、セキュリティの目標レベルが、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として設定された場合、セキュリティ評価部１１２は、図１１に示すＧＵＩ画面に表示

された機器および環境各々（つまり、WWWサーバ、クライアントおよび運用の各々）について、施策種別毎に、当該種別に分類されるセキュリティ施策数に対する実施済（つまり、実施有無入力欄にチェックが入れられた）セキュリティ施策数の割合を求める（ステップＳ１０１３）。そして、入出力制御部１１３を介して、表示装置１７に、その結果であるセキュリティ評価を表示する（ステップＳ１０１４）。

【００５４】

図１３は、セキュリティの目標レベルが施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として設定された場合における、セキュリティ評価結果の表示例を示している。この例では、図１２に示すＧＵＩ画面において、目標値として８０％以上が設定された場合を示している。ここで、WWWサーバ、クライアントおよび運用各々のセキュリティ評価結果は、別々に表示されるようになっており、操作者は入力装置１６を使ってタグ９１３を選択することにより、所望のセキュリティ評価結果を表示することができる。

【００５５】

また、図１３に示す例では、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合を、各施策種別を軸とする、いわゆるレーダチャートを用いて表示している。ここで、実線は、各軸上における、当該軸が示す施策種別のセキュリティ施策数に対する実施済のセキュリティ施策数の割合に応じた点を結んだ線、すなわちセキュリティ評価結果を示している。一方、一点鎖線は、各軸上における、図１２に示すＧＵＩ画面で設定された目標値に応じた点を結んだ線である。操作者は、セキュリティ評価結果を示す実線と目標レベルを示す一点鎖線を比較することで、視覚的に、対象システムに施されたセキュリティの状態を把握することが可能となる。

【００５６】

なお、ステップＳ１０１１において、設定されたセキュリティの目標レベルが、施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合であり、かつ、オプションとして特定業界における基準を適用するように設定された場合は、ステップＳ１０１３において、図１１に示すＧＵＩ画面に表示され

た機器および環境各々について、施策種別毎に、当該種別に分類されるセキュリティ施策のうち当該業界基準として義務付けらているセキュリティ施策数に対する実施済の当該業界基準として義務付けらているセキュリティ施策数の割合が求められる。

【００５７】

また、たとえば、ステップＳ１０１１において、セキュリティの目標レベルが、施策種別毎の実施済のセキュリティ施策による所要コストの総額として設定された場合、セキュリティ評価部１１２は、図１１に示すＧＵＩ画面に表示された機器および環境各々について、施策種別毎に、当該種別に分類されるセキュリティ施策のうち実施済セキュリティ施策による所要コストの総額を求める（ステップＳ１０１５）。そして、入出力制御部１１３を介して、表示装置１７に、その結果であるセキュリティ評価を表示する（ステップＳ１０１６）。

【００５８】

図１４は、セキュリティの目標レベルが施策種別毎の実施済のセキュリティ施策による所要コストの総額として設定された場合における、セキュリティ評価結果の表示例を示している。この例では、図１２に示すＧＵＩ画面において、目標値として１００万未満／年が設定された場合を示している。また、図１４に示す例では、図１３と同様、施策種別毎の実施済のセキュリティ施策による所要コストの総額を、各施策種別を軸とする、いわゆるレーダチャートを用いて表示している。ここで、実線は、各軸上における、当該軸が示す施策種別の実施済のセキュリティ施策による所要コストの総額に応じた点を結んだ線、すなわちセキュリティ評価結果を示している。一方、一点鎖線は、各軸上における、図１２に示すＧＵＩ画面で設定された目標値に応じた点を結んだ線である。操作者はセキュリティ評価結果を示す実線と目標レベルを示す一点鎖線を比較することで、視覚的に、対象システムに施されたセキュリティの状態を把握することが可能となる。

【００５９】

また、たとえば、ステップＳ１０１１において、セキュリティの目標レベルが、施策種別毎の未実施のセキュリティ施策による残存リスクの総額として設定された場合、セキュリティ評価部１１２は、図１１に示すＧＵＩ画面に表示された

機器および環境各々について、施策種別毎に、当該種別に分類されるセキュリティ施策のうち未実施のセキュリティ施策による残存リスクの総額を求める（ステップＳ１０１７）。そして、入出力制御部１１３を介して、表示装置１７に、その結果であるセキュリティ評価を表示する（ステップＳ１０１８）。

【００６０】

図１５は、セキュリティの目標レベルが施策種別毎の未実施のセキュリティ施策による残存リスクの総額として設定された場合における、セキュリティ評価結果の表示例を示している。この例では、図１２に示すＧＵＩ画面において、目標値として１００万未満／年が設定された場合を示している。また、図１５に示す例では、図１３と同様、施策種別毎の未実施のセキュリティ施策による残存リスクの総額を、各施策種別を軸とする、いわゆるレーダチャートを用いて表示している。ここで、実線は、各軸上における、当該軸が示す施策種別の未実施のセキュリティ施策による残存リスクの総額に応じた点を結んだ線、すなわちセキュリティ評価結果を示している。一方、一点鎖線は、各軸上における、図１２に示すＧＵＩ画面で設定された目標値に応じた点を結んだ線である。操作者はセキュリティ評価結果を示す実線と目標レベルを示す一点鎖線を比較することで、視覚的に、対象システムに施されたセキュリティの状態を把握することが可能となる。

【００６１】

以上、本発明の第１実施形態について説明した。

【００６２】

本実施形態では、図９に示すＧＵＩ画面において、操作者が、入力装置１６を用いて、対象システムの構成機器を指定して評価ボタンを選択すると、図１１に示すような、指定された機器毎にその機器に施すべきセキュリティ施策リストを含んだＧＵＩ画面が表示装置１７に表示される。操作者は、表示装置１７に表示された各機器のセキュリティ施策を見て、入力装置１６を用いて、実施有無入力欄にチェックする（いわゆるチェックリスト形式）ことで、そのセキュリティ施策の実施の有無を入力することができる。操作者が、入力装置１６を用いて、表示装置１７に表示された各機器のセキュリティ施策の実施の有無を入力すると、それに基づいて、対象システムに施されたセキュリティ施策の評価を行ない、そ

の結果を表示装置１７に表示する。

【００６３】

このように、本実施形態によれば、操作者がセキュリティを評価すべき対象システムの構成機器を指定するだけで、その構成機器各々に施すべきセキュリティ施策が表示される。そして、操作者が表示されている各構成機器のセキュリティ施策の実施の有無を入力するだけで、その評価対象システムに施されているセキュリティの評価を行なうことができる。したがって、操作者は、高度な専門的知識がなくても、システムのセキュリティ状態を評価することが可能となる。

【００６４】

また、本実施形態では、図１２に示すＧＵＩ画面において、操作者はセキュリティの目標レベルを設定することができる。また、図１３～図１５に示すように、セキュリティ評価結果は、設定した目標レベルと対比できるようにして表示される。このため、操作者は、評価対象システムの規模や評価対象システムに要求されるセキュリティレベルなどの、当該評価対象システムに固有の事情が考慮されたセキュリティ評価結果を得ることができる。

【００６５】

また、本実施形態では、図９に示すＧＵＩ画面において、操作者が、入力装置１６を用いて、対象システムの構成機器を指定して構築支援ボタンを選択すると、図１０に示すような、指定された機器毎にその機器に施すべきセキュリティ施策リストを含んだＧＵＩ画面が表示装置１７に表示される。このように本実施形態によれば、操作者がセキュリティ施策を構築すべき対象システムの構成機器を指定するだけで、その構成機器各々に施すべきセキュリティ施策が表示されるので、操作者は、高度な専門的知識がなくても、システムに施すべきセキュリティ施策を構築することが可能となる。

【００６６】

また、図９に示すＧＵＩ画面において選択されたセキュリティ強度以下のセキュリティ施策が図１０に示すセキュリティ施策リストに表示されるので、操作者は、対象システムの規模や対象システムに要求されるセキュリティレベルなどの、当該対象システムに固有の事情が考慮して、当該システムに施すべきセキュリ

ティ施策のリストを表示させることができる。

【００６７】

次に、本発明の第２実施形態について説明する。

【００６８】

図１６は、本発明の第２実施形態が適用されたセキュリティ支援・評価システムの概略図である。

【００６９】

上記の第１実施形態では、セキュリティ施策データベースDB_1～DB_n１３１を、セキュリティ支援・評価装置１の外部記憶装置１３に格納した場合について説明した。これに対し、本実施形態では、図１６に示すように、セキュリティ支援・評価装置１がたとえば携帯型の電子計算機上に構築される場合を考慮し、セキュリティ施策データベースDB_1～DB_n１３１をセキュリティ支援・評価装置１とは別の電子計算機上に構築されたデータベース管理装置2_1～2_n（$n \geqq 1$）に格納し、セキュリティ支援・評価装置１は、公衆網などのネットワークを介してデータベース管理装置2_i（$1 \leqq i \leqq n$）にアクセスし、セキュリティ施策リスト作成に必要な情報を得るようにしている。

【００７０】

図１７は、本発明の第２実施形態に用いるセキュリティ支援・評価装置１の概略構成図である。ここで、図１に示す第１実施形態のセキュリティ支援・評価装置１と同じ機能を有するものには同じ符号を付している。

【００７１】

図示するように、本実施形態のセキュリティ支援・評価装置１が、図１に示す第１実施形態のセキュリティ支援・評価装置１と異なる点は、外部記憶装置１３にセキュリティ施策データベースDB_1～DB_n１３１が格納されていない点と、外部記憶装置１３に、ネットワークを介してデータベース管理装置2_1～2_nにアクセスするための通信プログラムＰＧ１３３、および、図１８に示すようなデータベース管理装置2_1～2_nの各々アクセス先（アドレス）が記述されたＤＢアドレス管理テーブル１３４が格納されている点である。ＣＰＵ１１は、通信プログラム１３３をメモリ１２上にロードし実行することで、通信部１８により公衆網

などのネットワークを介してデータベース管理装置2_1～2_nにアクセスし、データベース管理装置2_1～2_nの間の通信を実現するために必要な各種プロトコル群を処理する通信制御部１１４をプロセスとして実現する。

【００７２】

図１９は、本発明の第２実施形態に用いるデータベース管理装置2_i（$1 \leqq i \leqq n$）の概略構成図である。ここで、図１に示す第１実施形態のセキュリティ支援・評価装置１と同じ機能を有するものには同じ符号を付している。

【００７３】

図示するように、本実施形態のデータベース管理装置2_iは、図１７に示すセキュリティ支援・評価装置１と異なる点は、外部記憶装置１３に、ＤＢアドレス管理テーブル１３４および評価・構築支援プログラムＰＧ１３２に代えて、セキュリティ施策データベースDB_i１３１およびＤＢ管理プログラムＰＧ１３５が格納されている点である。ＣＰＵ１１は、ＤＢ管理プログラム１３５をメモリ１２上にロードし実行することで、通信制御部１１４を介して、セキュリティ支援・評価装置１より受け取った要求に応じて、外部記憶装置１３に格納されているセキュリティ施策データベースDB_i１３１から必要な情報を読み出し、セキュリティ支援・評価装置１に送信するデータベースＤＢ検索部１１５をプロセスとして実現する。

【００７４】

次に、上記構成のセキュリティ支援・評価システムの動作について説明する。

【００７５】

まず、図１７に示すセキュリティ支援・評価装置１の動作について説明する。

【００７６】

本実施形態のセキュリティ支援・評価装置１の動作は、図６および図７に示す第１実施形態のセキュリティ支援・評価装置１の動作と基本的に同様である。ただし、以下の点で異なる。

【００７７】

すなわち、ステップＳ１００１において、セキュリティ支援・評価装置１は、データベース管理装置2_1～2_nが格納するセキュリティ施策データベースDB_1

～ＤＢ$_n$１３１各々の対象システムの名称を、予め外部記憶装置１３などに記憶しており、施策リスト生成部１１１は、外部記憶装置１３からセキュリティ施策データベースＤＢ$_1$～ＤＢ$_n$１３１の対象システム各々の名称を読み出し、入出力制御部１１３を用いて、図８に示すようなＧＵＩ画面を表示する。

【００７８】

また、ステップＳ１００３において、施策リスト生成部１１１は、ステップＳ１００２で選択されたシステムのセキュリティ施策データベースを格納するデータベース管理装置２$_i$より当該システムの構成機器の名称を読み出すため指示を通信制御部１１４に渡す。これを受けて、通信制御部１１４は、当該データベース管理装置２$_i$のアドレスを外部記憶装置１３に格納されているＤＢアドレス管理テーブル１３４から取得し、通信装置１８を介して、当該データベース管理装置２$_i$に指示を送信する。その後、通信制御部１１４は、当該データベース管理装置２$_i$から当該システムの構成機器の名称が送られてくると、これらを施策リスト生成部１１１に渡す。これを受けて、施策リスト生成部１１１は、入出力制御部１１３を用いて、受け取った構成機器の名称のリストを含んだ、図９に示すようなＧＵＩ画面を表示する。

【００７９】

さらに、ステップＳ１００５において、図２０に示す処理を行なう。

【００８０】

まず、施策リスト生成部１１１は、ステップＳ１００２で選択されたシステムのセキュリティ施策データベースを格納するデータベース管理装置２$_i$より必要な情報を読み出すための検索指示を、ステップＳ１００４にて図９に示すようなＧＵＩ画面を介して操作者によりチェックされた項目の内容とともに、通信制御部１１４に渡す（ステップＳ１１０１）。

【００８１】

これを受けて、通信制御部１１４は、当該データベース管理装置２$_i$のアドレスを外部記憶装置１３に格納されているＤＢアドレス管理テーブル１３４から取得し、通信装置１８を介して、当該データベース管理装置２$_i$に、前記チェックされた項目の内容を含んだデータベースの検索指示を送信する（ステップＳ１１

０２）。その後、通信制御部１１４は、当該データベース管理装置２$_i$から検索結果が送られてくると（ステップＳ１１０３）、これらを施策リスト生成部１１１に渡す。

【００８２】

これを受けて、施策リスト生成部１１１は、検索結果に基づいて、図９に示すＧＵＩ画面の項目「機器構成」８０１にてチェックされた機器および項目「環境」８０２にてチェックされた環境毎に、セキュリティ施策リストを作成する（ステップＳ１１０４）。

【００８３】

次に、図１９に示すデータベース管理装置２$_i$の動作について説明する。

【００８４】

図２１は、本発明の第２実施形態で用いるデータベース管理装置２$_i$の動作を説明するためのフロー図である。

【００８５】

まず、通信制御部１１４は、通信装置１８を介して、セキュリティ支援・評価装置１からシステムの構成機器の名称を読み出すため指示を受け取ると（ステップＳ２００１）、これをＤＢ検索部１１５に渡す。これを受けて、ＤＢ検索部１１５は、外部記憶装置１３に格納されているセキュリティ施策データベースＤＢ$_i$から、当該データベースの列２０６に記述されている各構成機器の名称を読み出し（図２～図５参照）、通信制御部１１４に渡す（ステップＳ２００２）。通信制御部１１４は、受け取った各構成機器の名称を、セキュリティ支援・評価装置１に送信する（ステップＳ２００３）。

【００８６】

次に、通信制御部１１４は、通信装置１８を介して、セキュリティ支援・評価装置１から、図９に示すＧＵＩ画面でチェックされた構成機器や環境の名称およびセキュリティ強度を含んだ検索指示を受け取ると（ステップＳ２００４）、これをＤＢ検索部１１５に渡す。これを受けて、ＤＢ検索部１１５は、外部記憶装置１３に格納されているセキュリティ施策データベースＤＢ$_i$から必要な情報を読み出す（ステップＳ２００５）。

【００８７】

たとえば、外部記憶装置１３に格納されているセキュリティ施策データベースＤＢ$_i$が図２および図３に示すインターネット接続システムのものであり、検索指示に含まれる構成機器および環境の名称が、「ＷＷＷサーバ」、「クライアント」および「運用」であり、セキュリティ強度が「並」であるる場合、以下のようにして必要な情報を読み出す。

【００８８】

まず、図２および図３に示すインターネット接続システムのデータベースの「ＷＷＷサーバ」の列２０６$_1$の各行において、同じ行のセキュリティ施策が適用可能であり、かつ、当該セキュリティ施策を適用した場合に確保されるセキュリティレベルが、検索指示に含まれるセキュリティ強度（ここでは「並」＝Ｌ１）以下のものが記述された行に着目する。そして、着目した各行について、「ＷＷＷサーバ」の列２０６$_1$に記述された内容と同じ行の列２０１～２０４、２０５$_i$に記述された内容とを読み出す。以上の処理を、「クライアント」の列２０６$_2$および「運用」の列２０８のそれぞれに対しても、同様に実行することで、検索指示に含まれる構成機器および環境毎に、必要な情報を読み出す。

【００８９】

次に、ＤＢ検索部１１５は、上記のようにして読み出した情報を通信制御部１１４に渡す。通信制御部１１４は、受け取った情報を、検索結果として、セキュリティ支援・評価装置１に送信する（ステップＳ２００６）。

【００９０】

以上、本発明の第２実施形態について説明した。

【００９１】

本実施形態では、セキュリティ施策データベースＤＢ$_1$～ＤＢ$_n$１３１をセキュリティ支援・評価装置１とは別の電子計算機上に構築されたデータベース管理装置２$_1$～２$_n$に格納し、セキュリティ支援・評価装置１は、公衆網などのネットワークを介してデータベース管理装置２$_i$にアクセスし、セキュリティ施策リスト作成に必要な情報を得るようにしているので、セキュリティ支援・評価装置１を、たとえば携帯型の電子計算機上に構築する場合に好適である。

【００９２】

なお、上記の実施形態において、セキュリティ支援・評価装置１は、データベース管理装置2_1～2_nが格納するセキュリティ施策データベースDB_1～DB_n１３１各々の対象システムの名称を、予め外部記憶装置１３などに記憶しておくようにしているが、この情報は、セキュリティ支援・評価装置１がデータベース管理装置2_1～2_n各々に定期的にアクセスすることで、取得するようにしてもよい。また、この際、各データベース管理装置2_1～2_nから、セキュリティ施策データベースの対象システムの名称とともに当該対象システムの構成機器の名称も併せて取得しておくようにすれば、上述した図６のステップＳ１００３の変更は不要になる。

【００９３】

【発明の効果】

以上説明したように、本発明によれば、高度な専門的知識がなくても、システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援することが可能になる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態が適用されたセキュリティ支援・評価装置１の概略構成図である。

【図２】

インターネット接続システムに対応するセキュリティ施策データベースの一例を示す図である。

【図３】

インターネット接続システムに対応するセキュリティ施策データベースの一例を示す図である。

【図４】

認証システムに対応するセキュリティ施策データベースの一例を示す図である。

【図５】

プラントシステムに対応するセキュリティ施策データベースの一例を示す図である。

【図６】

本発明の第１実施形態であるセキュリティ支援・評価装置１の動作を説明するためのフロー図である。

【図７】

本発明の第１実施形態であるセキュリティ支援・評価装置１の動作を説明するためのフロー図である。

【図８】

セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの名称を選択するためのＧＵＩ画面の例を示した図である。

【図９】

セキュリティ施策の作成支援あるいはセキュリティ状態の評価の対象となるシステムの構成機器の選択するためのＧＵＩ画面の例を示した図である。

【図１０】

セキュリティ施策の作成支援のために表示されるセキュリティ施策リストの一例を示した図である。

【図１１】

セキュリティ評価のために表示されるセキュリティ施策の実施の有無を確認するためのＧＵＩ画面の一例を示した図である。

【図１２】

操作者より達成すべきセキュリティの目標レベルを受け付けるためのＧＵＩ画面の例を示した図である。

【図１３】

セキュリティの目標レベルが施策種別毎のセキュリティ施策数に対する実施済のセキュリティ施策数の割合として設定された場合における、セキュリティ評価結果の表示例を示す図である。

【図１４】

セキュリティの目標レベルが施策種別毎の実施済のセキュリティ施策による所要コストの総額として設定された場合における、セキュリティ評価結果の表示例を示す図である。

【図１５】

セキュリティの目標レベルが施策種別毎の未実施のセキュリティ施策による残存リスクの総額として設定された場合における、セキュリティ評価結果の表示例を示す図である。

【図１６】

本発明の第２実施形態が適用されたセキュリティ支援・評価システムの概略図である。

【図１７】

本発明の第２実施形態に用いるセキュリティ支援・評価装置１の概略構成図である。

【図１８】

本発明の第２実施形態に用いるセキュリティ支援・評価装置１の外部記憶装置１３に格納されているＤＢアドレス管理テーブル１３４を説明するための図である。

【図１９】

本発明の第２実施形態に用いるデータベース管理装置2_i（$1 \leqq i \leqq n$）の概略構成図である。

【図２０】

本発明の第２実施形態に用いるセキュリティ支援・評価装置１における、図６のステップＳ１００５の処理を説明するためのフロー図である。

【図２１】

本発明の第２実施形態で用いるデータベース管理装置2_iの動作を説明するためのフロー図である。

【符号の説明】

１･･･セキュリティ支援・評価装置

2_1～2_n･･･データベース管理装置

１１･･･ＣＰＵ

１２･･･メモリ

１３･･･外部記憶装置

１４･･･読取り装置

１５･･･過般性のある記憶媒体

１６･･･入力装置

１７･･･表示装置

１８･･･通信装置

１９･･･インターフェース

１１１･･･施策リスト生成部

１１２･･･セキュリティ評価部

１１３･･･入出力制御部

１１４･･･通信制御部

１１５･･･ＤＢ検索部

１３１･･･セキュリティ施策データベースDB_1～DB_n

１３２･･･評価・構築支援プログラムＰＧ

１３３･･･通信プログラムＰＧ

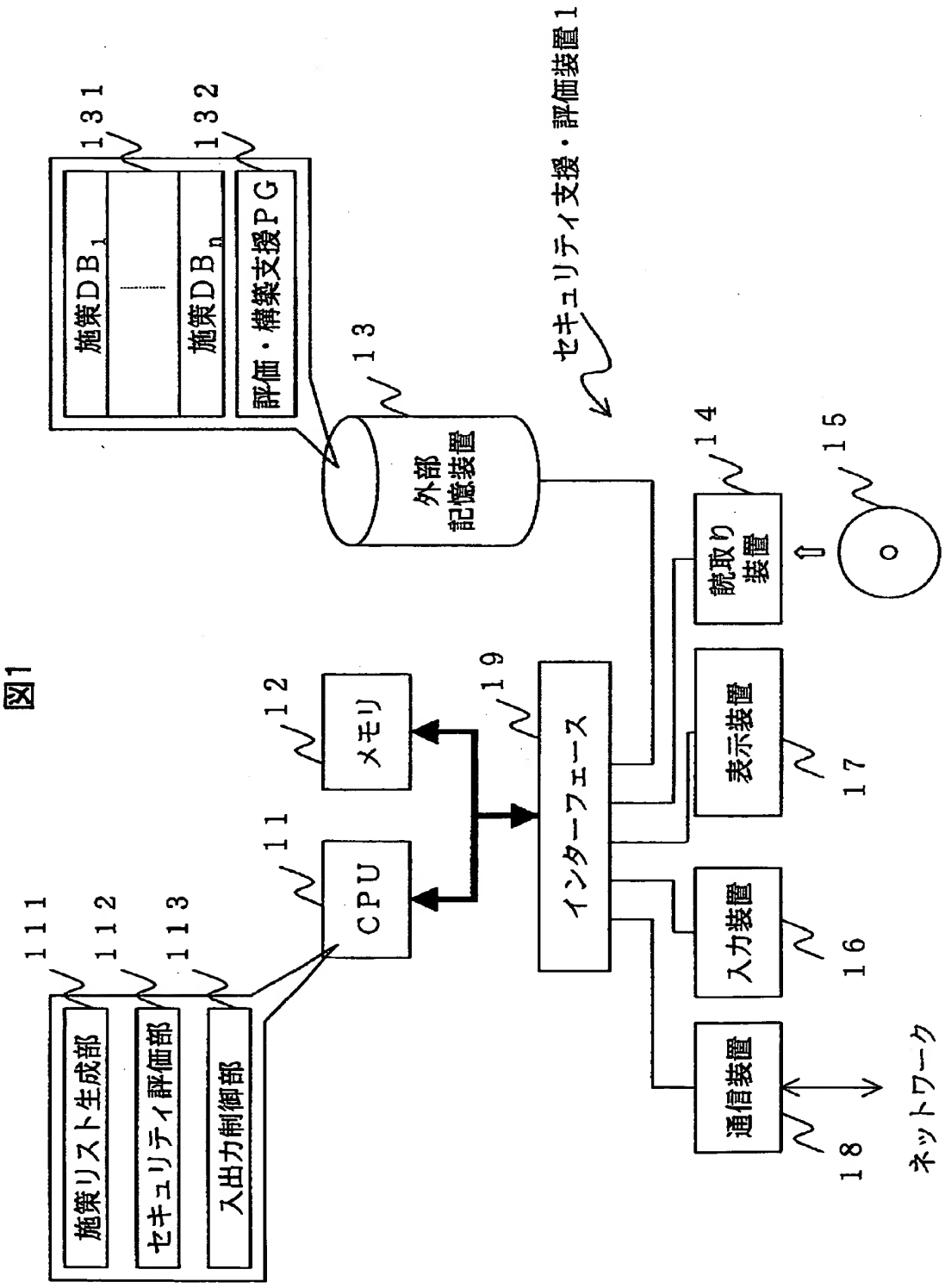
１３４･･･データベースアドレステーブル

１３５･･･データベース管理プログラムＰＧ

【書類名】　図面

【図１】

図1


セキュリティ支援・評価装置1
131
132
施策DB1
施策DBn
評価・構築支援PG
13
外部記憶装置
14
読取り装置
15
12
メモリ
19
インターフェース
表示装置
17
11
CPU
111
112
113
施策リスト生成部
セキュリティ評価部
入出力制御部
入力装置
16
通信装置
18
ネットワーク

【図2】

インターネット接続システム（その1）

図2

201	202	203	204	205₁	205₂	206₁	206₂	206₃	207	208
施策種別	セキュリティ施策	想定脅威	CC機能要件	業種A基準	業種B基準	WWWサーバ	クライアント	ボーダルータ	施設	運用
アクセス権限の管理	アクセス権限の管理者を設定	不正使用		◎	◎					L2,C2,R4
アクセス権限の管理	個人単位でパスワードを設定	不正使用	FMT_MSA.1			L3,C2,R2	L3,C2,R2			
アクセス権限の管理	アクセス権限の設定状況を随時確認可能に設定	不正使用	FMT_MSA.1 FMT_MTD.1			L2,C2,R3	L2,C2,R3			
アクセス権限の管理	アクセスを特権ユーザに限定	情報漏洩	FDP_ACF.1 FDP_ACC.2 FIA_UAU.1	◎		L1,C2,R3	L3,C1,R3			
アクセス権限の管理	管理ユティリティの利用可能者を限定	情報漏洩	FDP_ACC.1 FDP_ACF.1			L1,C1,R3	L1,C1,R3	L1,C1,R3		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
識別と認証	リモートアクセスで特権ユーザになれる端末限定	不正使用	FIA_UAU.2 FIA_UID.1	◎		L3,C3,R3		L2,C4,R3		
識別と認証	IPアドレスで相手を確認	不正使用				L2,C2,R3		L1,C2,R3		
識別と認証	認証失敗時に各種情報を表示せず	不正使用	FIA_AFL.1 FIA_UAU.7			L1,C1,R2	L1,C2,R2	L1,C2,R2		
識別と認証	1回の認証失敗でユーザIDをロック	不正使用	FIA_AFL.1			L2,C3,R3		L1,C3,R3		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

セキュリティレベル
L1:並,L2:強,L3:最強

年間所要コスト
C1:10万未満,C2:100万未満,C3:500万未満,
C4:1000万未満,C5:1000万以上

年間残存リスク
R1:10万未満,R2:100万未満,R3:500万未満
R4:1000万未満,R5:1000万以上

出証特2000-3033830

インターネット接続システム（その2）

図3

【図3】

201 施策種別	202 セキュリティ施策	203 想定脅威	204 CC機能要件	205₁ 業種A基準	205₂ 業種B基準	206₁ WWWサーバ	206₂ クライアント	206₃ ボーダルータ	207 施設	208 運用
ウイルス対策	ウイルスチェッカを定期的に起動	情報改竄				L3,C2,R3	L1,C1,R3			
ウイルス対策	ウイルス定義を定期的に更新	情報改竄				L3,C2,R3	L1,C1,R2			
ウイルス対策	ＦＤ等の可搬性記憶媒体を使用不可に設定	情報改竄				L3,C1,R2	L3,C1,R2			
ウイルス対策	デーモン起動機構を定期的にチェック	情報改竄				L3,C3,R3				
ウイルス対策	不要なサービスを停止	不正使用				L2,C2,R3	L1,C2,R3			
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
入退室管理	出入り口に施錠	機器破壊		◎					L1,C4,R4	
入退室管理	入室に必要な鍵等を所定場所に管理・管理	機器破壊								L2,C2,R4
入退室管理	入室許可証を発行	機器破壊								L2,C2,R4
入退室管理	入室管理にレベルを設定	機器破壊								L3,C3,R4
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

セキュリティレベル
L1:並,L2:強,L3:最強

年間所要コスト
C1:10万未満,C2:100万未満,C3:500万未満,
C4:1000万未満,C5:1000万以上

年間残存リスク
R1:10万未満,R2:100万未満,R3:500万未満
R4:1000万未満,R5:1000万以上

出証特２０００－３０３３８３０

特平１１－２７７２６５

【図4】

認証システム

図4

201 施策種別	202 セキュリティ施策	203 想定脅威	204 CC機能要件	205₁ 業種A基準	205₂ 業種B基準	206₁ 認証サーバ	206₂ 暗号装置	206₃ ルータ	207 施設	208 運用
認証書管理	認証書の有効期限を設定	不正使用	FMT_SAE.1 FMT_MSA.1			L1,C3,R4				
認証書管理	認証書を無効にする前に本人の識別・認証を実行	不正使用	FIA_UID.2 FIA_UAU.1			L2,C3,R4	L1,C3,R4			
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
鍵管理	不許可になった鍵へのアクセスを監査証跡に記録	不正使用	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3			L2,C3,R5	L1,C3,R5	L3,C3,R5		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
侵入者対策	外部ネットワークとの接続点にファイアウォール	情報漏洩							L1,C4,R5	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
入退室管理	資格変更に伴う許可証の変更・回収を迅速に	機器破壊								L2,C4,R5
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

セキュリティレベル
L1:並,L2:強,L3:最強

年間所要コスト
C1:10万未満,C2:100万未満,C3:500万未満,
C4:1000万未満,C5:1000万以上

年間残存リスク
R1:10万未満,R2:100万未満,R3:500万未満
R4:1000万未満,R5:1000万以上

出証特2000-3033830

【図5】

プラントシステム

図5

201 施策種別	202 セキュリティ施策	203 想定脅威	204 CC機能要件	205₁ 業種A基準	205₂ 業種B基準	206₁ 制御装置	206₂ 管理装置	206₃ ファイアウォール	207 施設	208 運用
プラント操作権限管理	操作前に、本人の識別・認証を実行	不正使用	FIA_UID.2 FMT_UAU.1			L2,C3,R4	L1,C3,R4	L1,C3,R4		
プラント操作権限管理	技術レベルを考慮してユーザに特権を付与	不正使用	FMT_MSA.1							L1,C3,R4
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
プラント操作監視	不許可になった操作を監査証跡に記録	不正使用	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3			L2,C3,R5	L1,C3,R5	L3,C3,R5		
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
侵入者対策	外部ネットワークとの接続点にファイアウォール	情報漏洩							L1,C4,R5	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
入退室管理	入室管理にレベルを設定	機器破壊								L2,C4,R5
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

セキュリティレベル
L1:並,L2:強,L3:最強

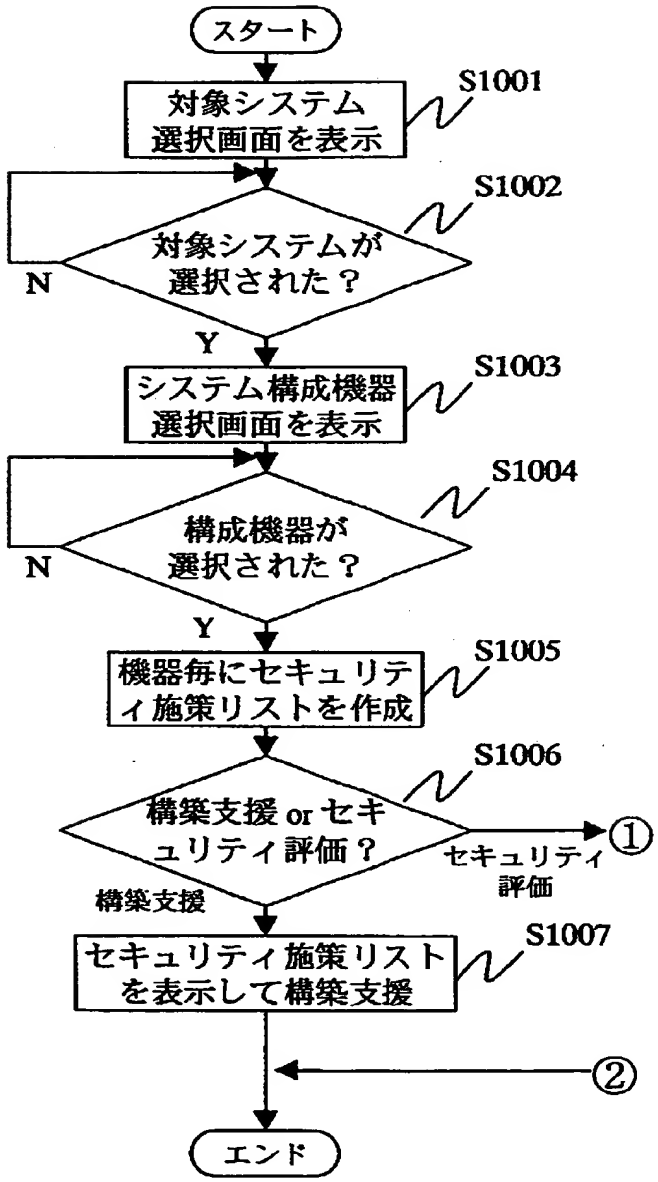
年間所要コスト
C1:10万未満,C2:100万未満,C3:500万未満,
C4:1000万未満,C5:1000万以上

年間残存リスク
R1:10万未満,R2:100万未満,R3:500万未満
R4:1000万未満,R5:1000万以上

出証特2000－3033830

【図６】

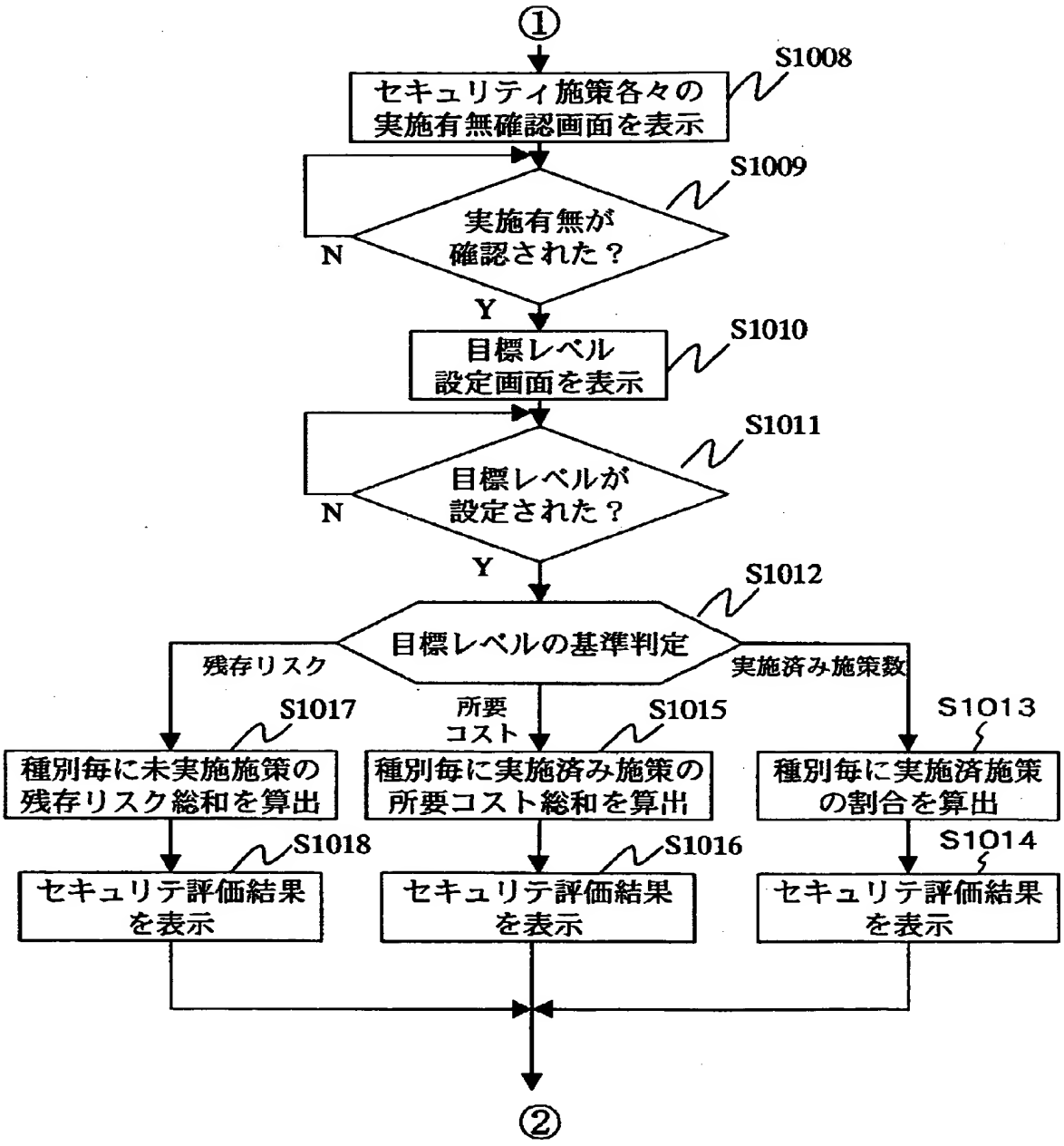
図６



出証特２０００－３０３３８３０

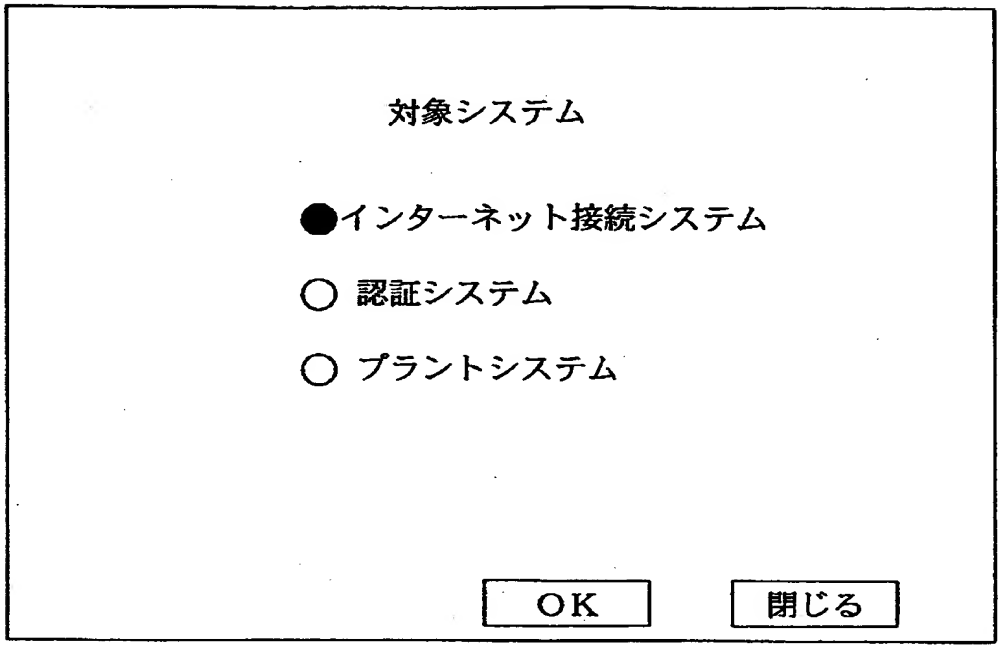
【図７】

図７


①
S1008
セキュリティ施策各々の
実施有無確認画面を表示
S1009
実施有無が
確認された？
N
Y
S1010
目標レベル
設定画面を表示
S1011
目標レベルが
設定された？
N
Y
S1012
目標レベルの基準判定
残存リスク
所要
コスト
実施済み施策数
S1017
種別毎に未実施施策の
残存リスク総和を算出
S1015
種別毎に実施済み施策の
所要コスト総和を算出
S1013
種別毎に実施済施策
の割合を算出
S1018
セキュリテ評価結果
を表示
S1016
セキュリテ評価結果
を表示
S1014
セキュリテ評価結果
を表示
②

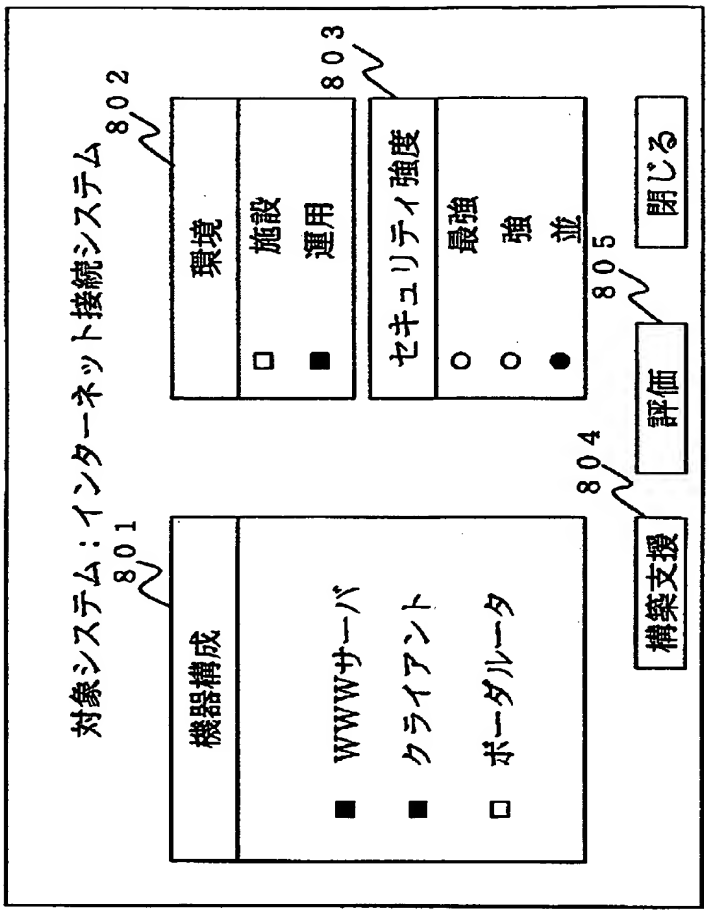
【図８】

図８



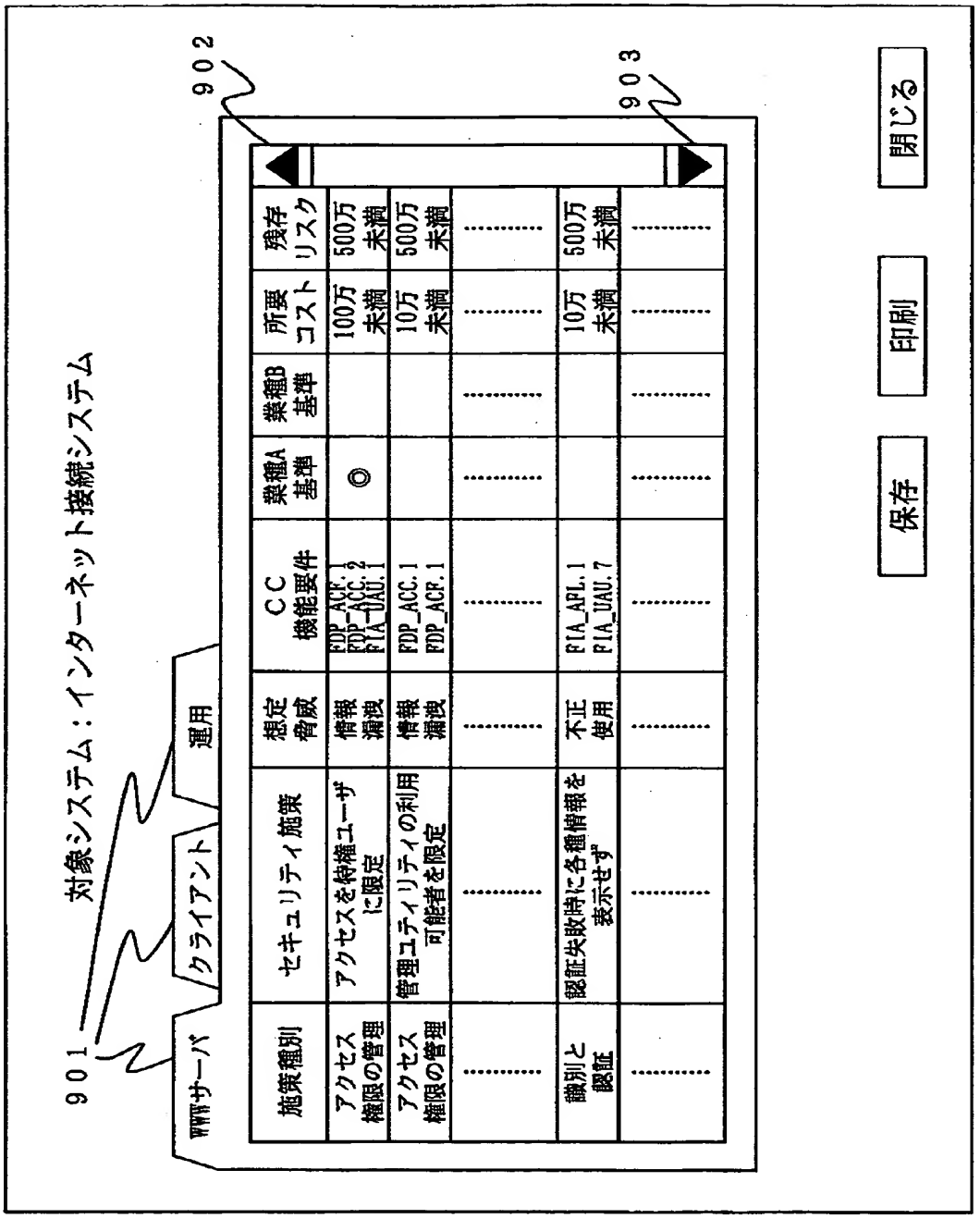
【図９】

図９


対象システム：インターネット接続システム
801
機器構成
WWWサーバ
クライアント
ボーダルータ
802
環境
施設
運用
803
セキュリティ強度
最強
強
並
804
構築支援
805
評価
閉じる

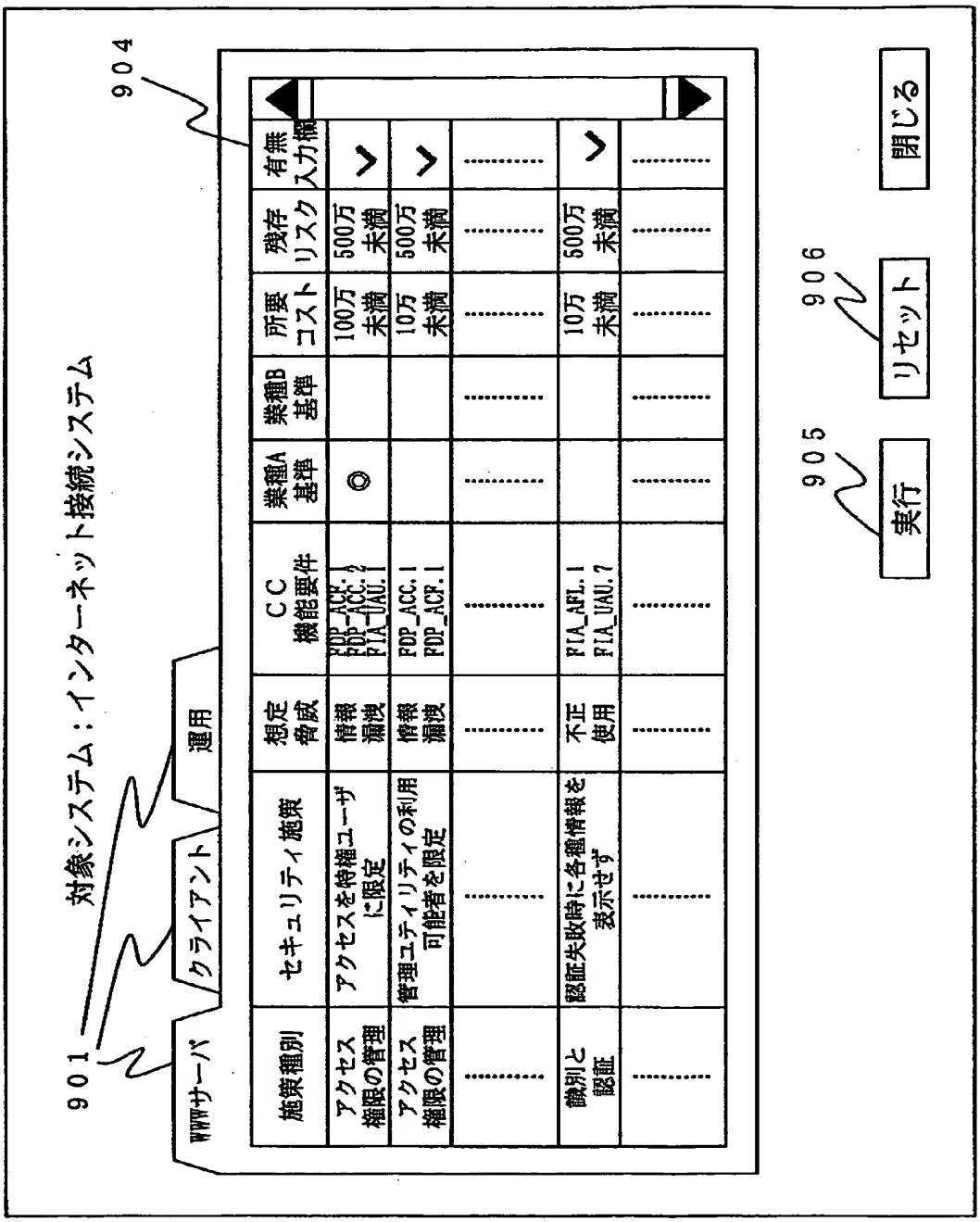
【図１０】

図１０


901
対象システム：インターネット接続システム
WWWサーバ
クライアント
運用
902
903
施策種別
セキュリティ施策
想定脅威
CC機能要件
業種A基準
業種B基準
所要コスト
残存リスク
アクセス権限の管理
アクセスを特権ユーザに限定
情報漏洩
FDP_ACF.1 FDP_ACC.2 FIA_UAU.1
◎
100万未満
500万未満
アクセス権限の管理
管理ユティリティの利用可能者を限定
情報漏洩
FDP_ACC.1 FDP_ACF.1
10万未満
500万未満
識別と認証
認証失敗時に各種情報を表示せず
不正使用
FIA_AFL.1 FIA_UAU.7
10万未満
500万未満
保存
印刷
閉じる

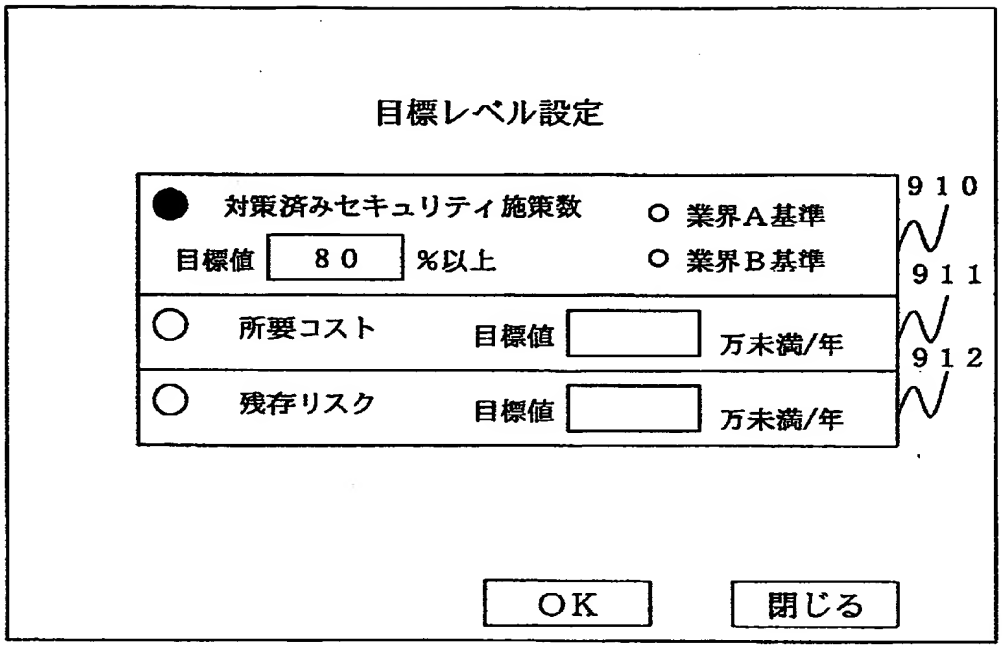
【図１１】

図１１


９０１
対象システム：インターネット接続システム
９０４
WWWサーバ
クライアント
運用
施策種別
セキュリティ施策
想定脅威
CC機能要件
業種A基準
業種B基準
所要コスト
残存リスク
有無入力欄
アクセス権限の管理
アクセスを特権ユーザに限定
情報漏洩
FDP_ACC.2 FDP_ACF.1 FIA_UAU.1
◎
100万未満
500万未満
アクセス権限の管理
管理ユティリティの利用可能者を限定
情報漏洩
FDP_ACC.1 FDP_ACF.1
10万未満
500万未満
識別と認証
認証失敗時に各種情報を表示せず
不正使用
FIA_AFL.1 FIA_UAU.7
10万未満
500万未満
９０５
実行
９０６
リセット
閉じる

【図１２】

図１２


目標レベル設定
対策済みセキュリティ施策数
業界Ａ基準
目標値
８０
％以上
業界Ｂ基準
９１０
９１１
所要コスト
目標値
万未満/年
９１２
残存リスク
目標値
万未満/年
ＯＫ
閉じる

【図１３】

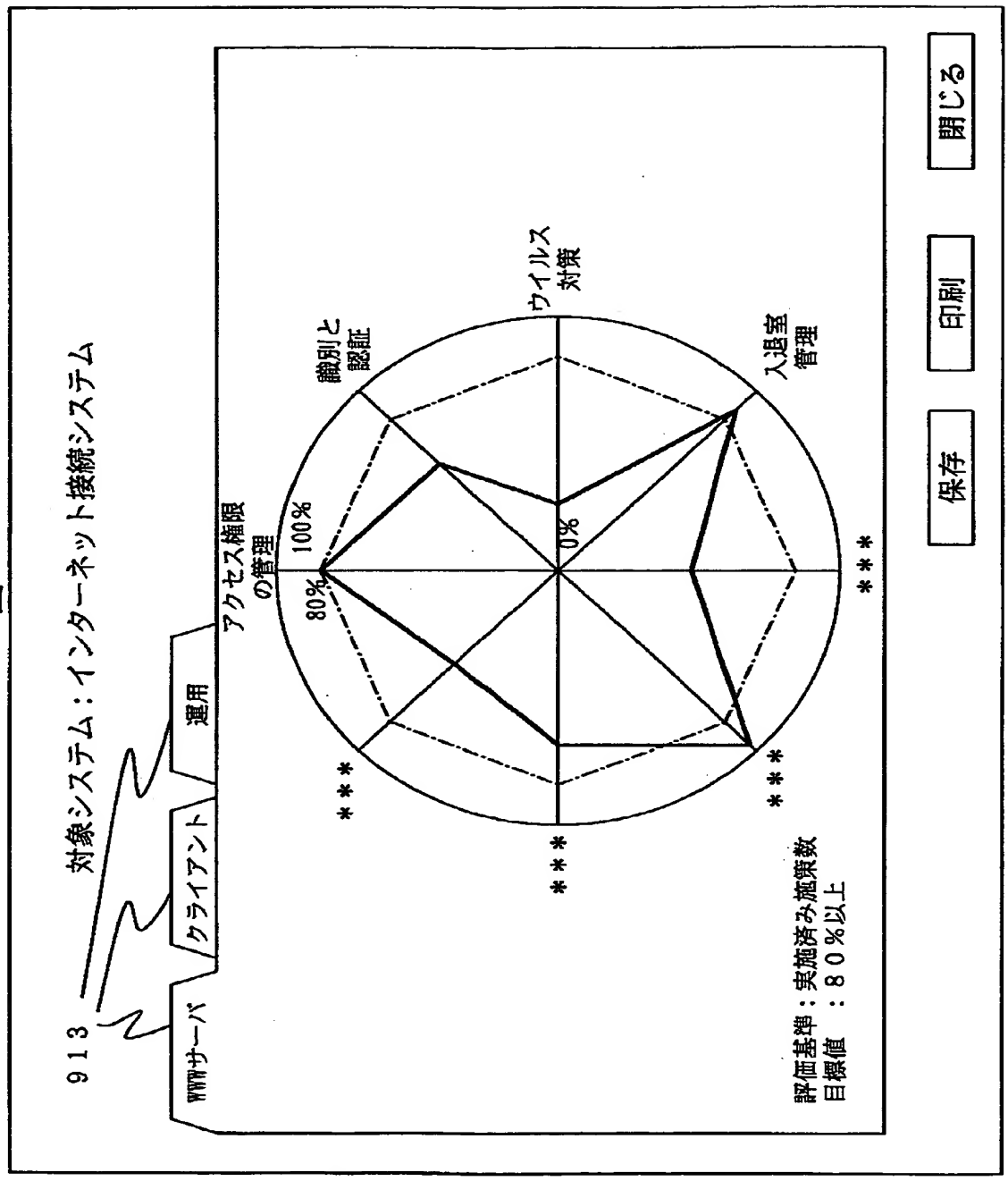


図13
対象システム：インターネット接続システム
913
WWWサーバ
クライアント
運用
アクセス権限の管理
識別と認証
ウイルス対策
入退室管理
100%
80%
0%
***
***
***
***
***
評価基準：実施済み施策数
目標値　：８０％以上
保存
印刷
閉じる

【図１４】

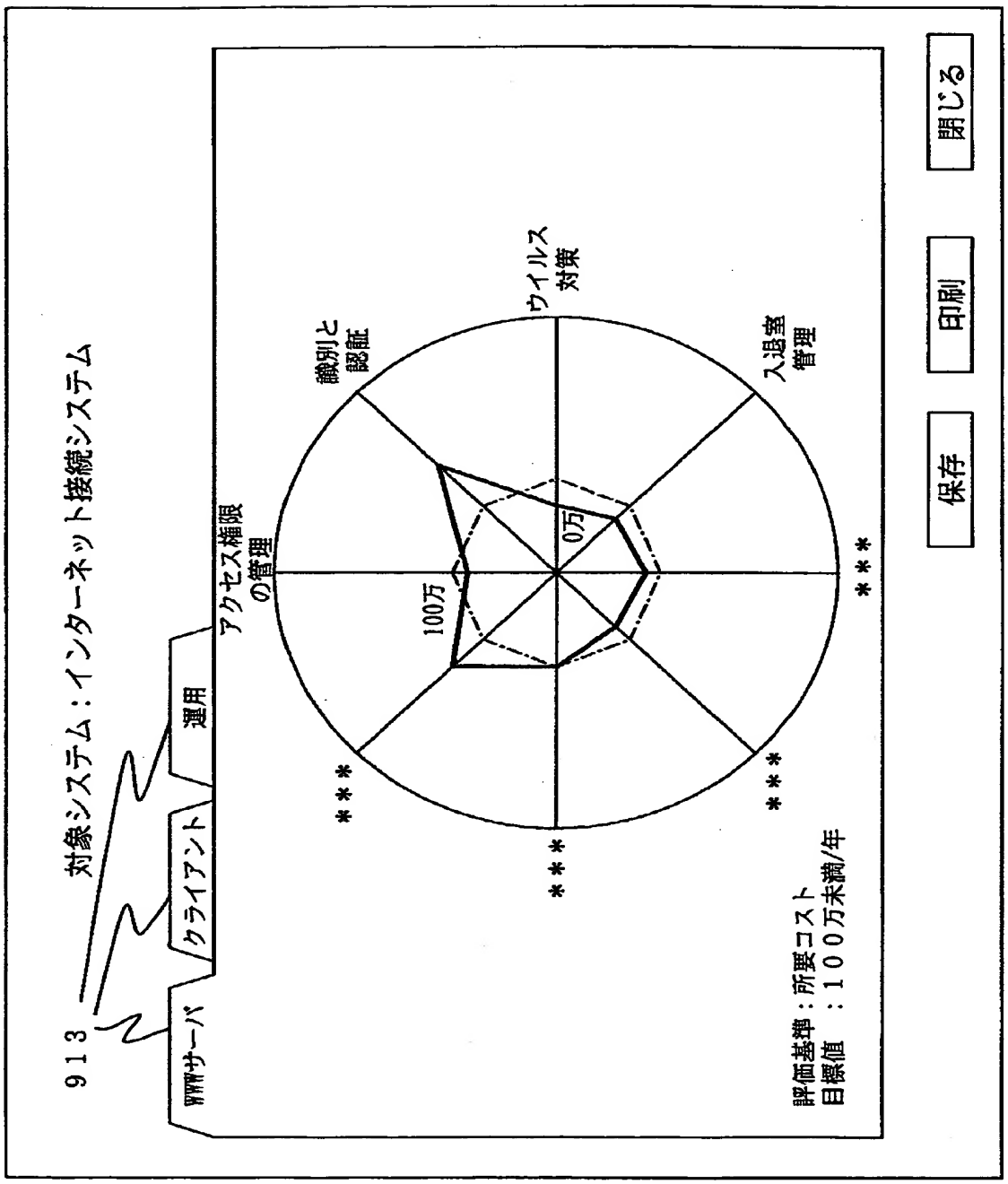


図14
対象システム：インターネット接続システム
913
WWWサーバ
クライアント
運用
アクセス権限の管理
識別と認証
ウイルス対策
入退室管理
100万
0万
＊＊＊
＊＊＊
＊＊＊
＊＊＊
＊＊＊
評価基準：所要コスト
目標値　：１００万未満/年
保存
印刷
閉じる

【図１５】

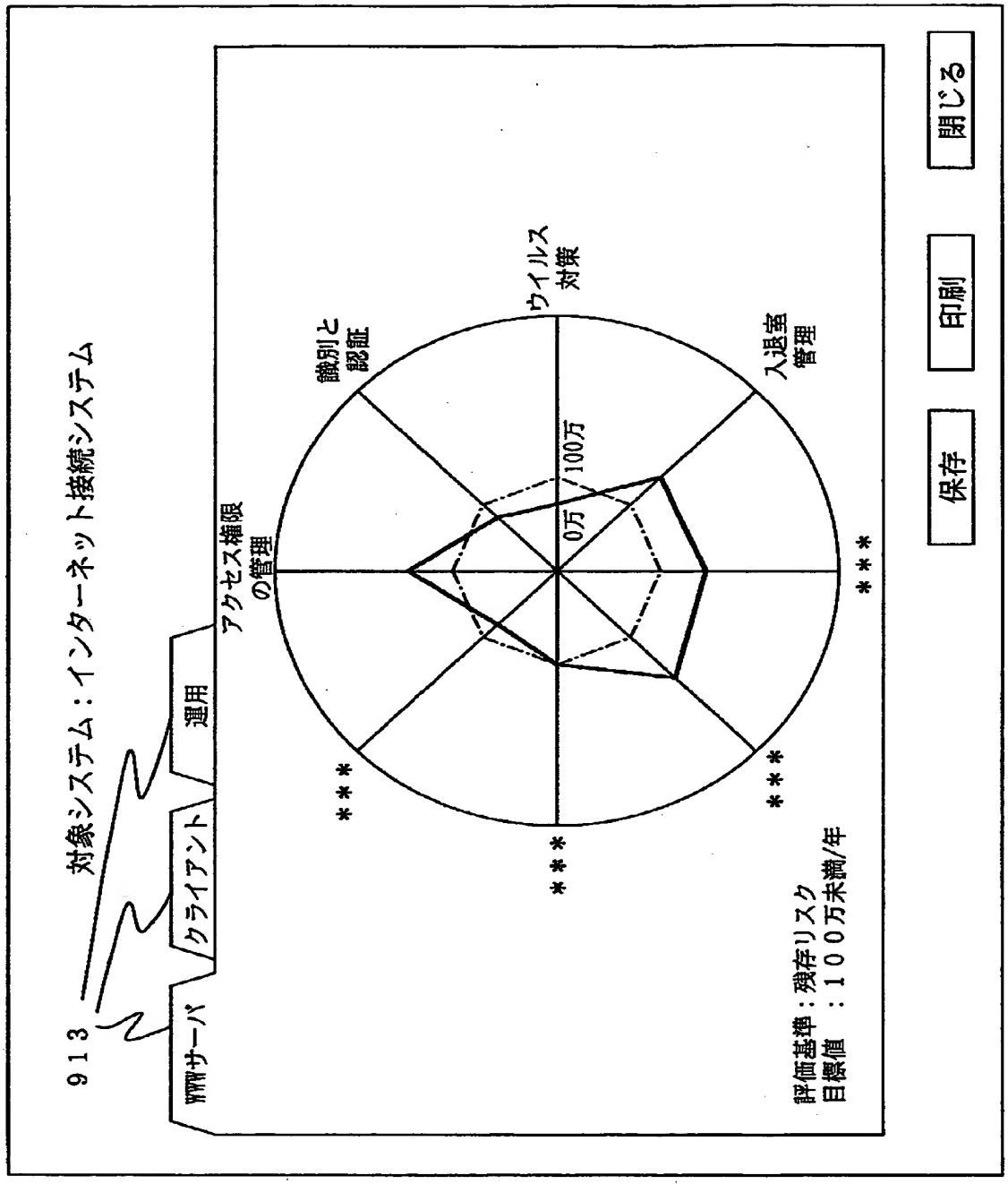
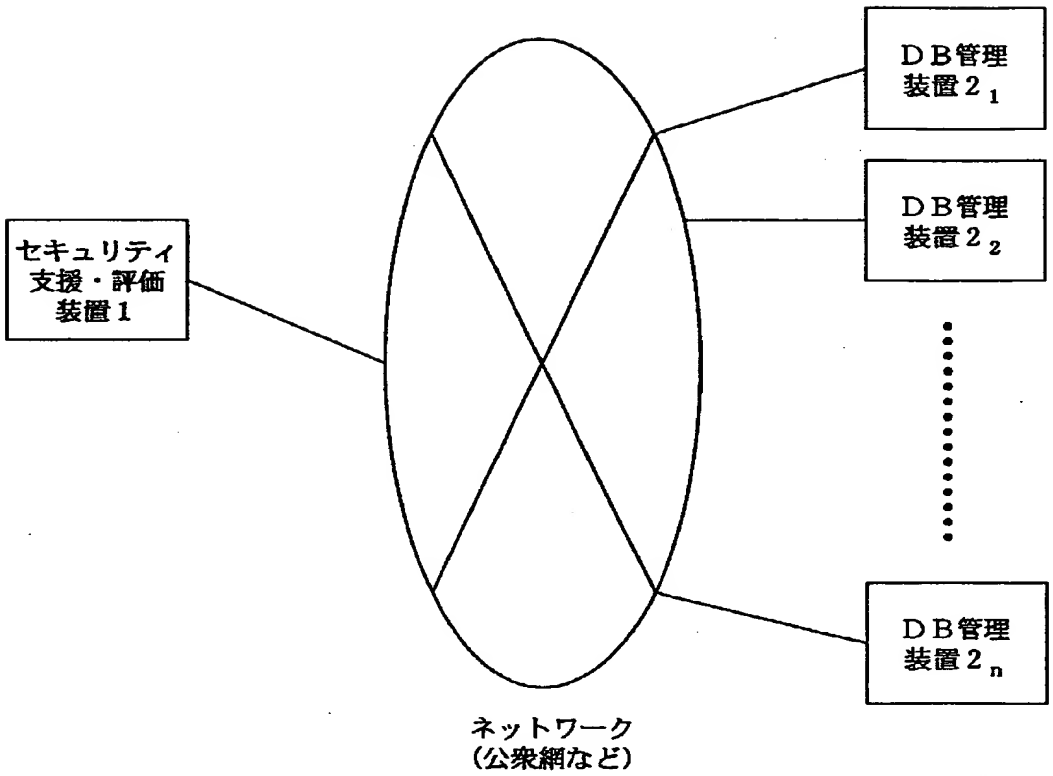


図15
対象システム：インターネット接続システム
913
WWWサーバ
クライアント
運用
アクセス権限の管理
識別と認証
ウイルス対策
入退室管理
0万
100万
＊＊＊
＊＊＊
＊＊＊
＊＊＊
評価基準：残存リスク
目標値　：１００万未満/年
保存
印刷
閉じる

【図１６】

図１６



【図１７】

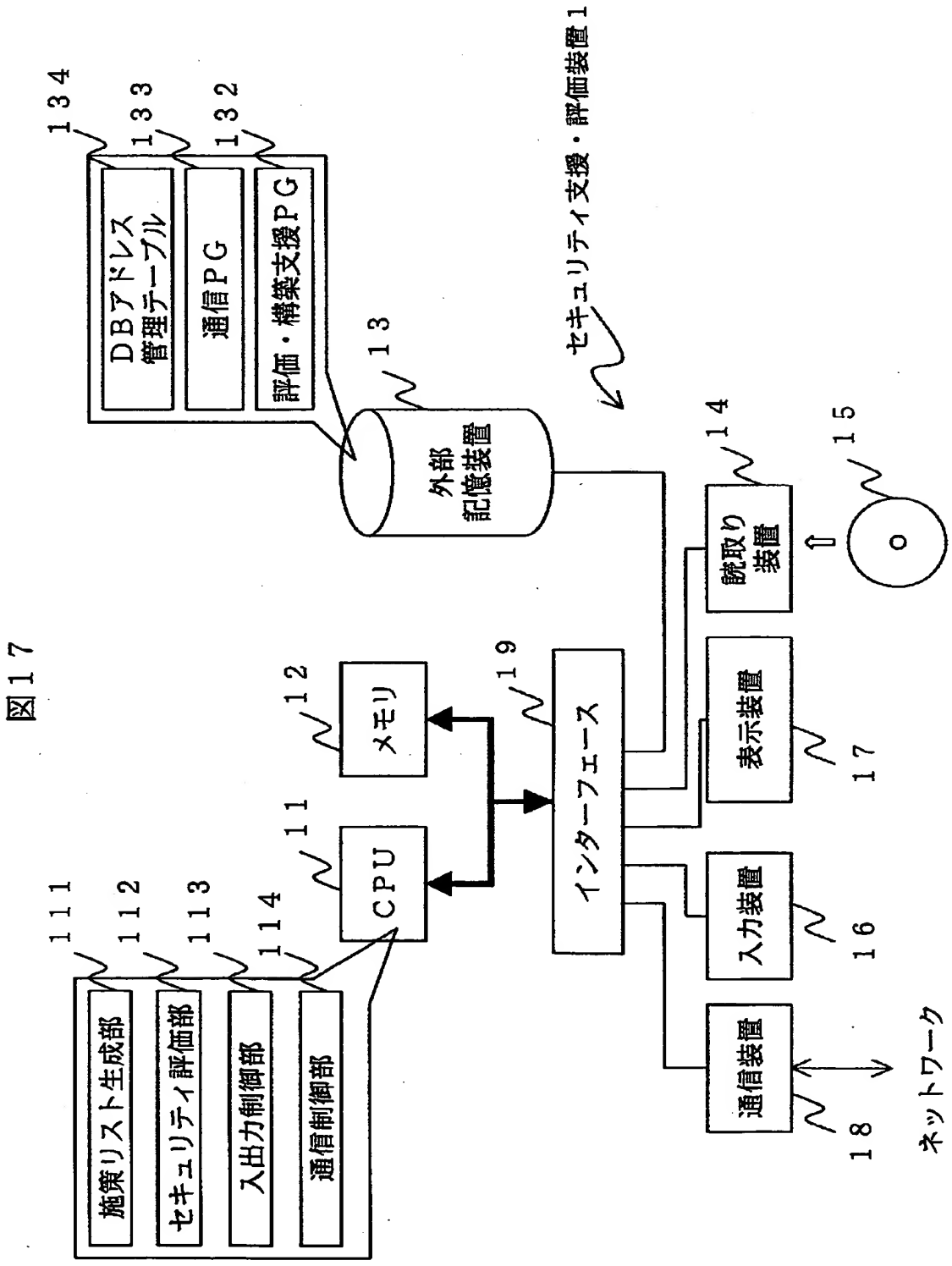

１３４
１３３
１３２
ＤＢアドレス管理テーブル
通信ＰＧ
評価・構築支援ＰＧ
１３
外部記憶装置
セキュリティ支援・評価装置１
１４
１５
読取り装置
メモリ
１２
１９
インターフェース
表示装置
１７
１１１
１１２
１１３
１１４
１１
ＣＰＵ
施策リスト生成部
セキュリティ評価部
入出力制御部
通信制御部
入力装置
１６
通信装置
１８
ネットワーク

図１７

【図１８】

図１８

施策ＤＢ （対象システム）	ＤＢ管理装置アドレス
施策DB_1 （インターネット接続システム）	****.***.**.**
施策DB_2 （認証システム）	****.***.**.**
施策DB_3 （プラントシステム）	****.***.**.**
⋮	⋮
施策DB_n （＊＊＊システム）	****.***.**.**

【図１９】

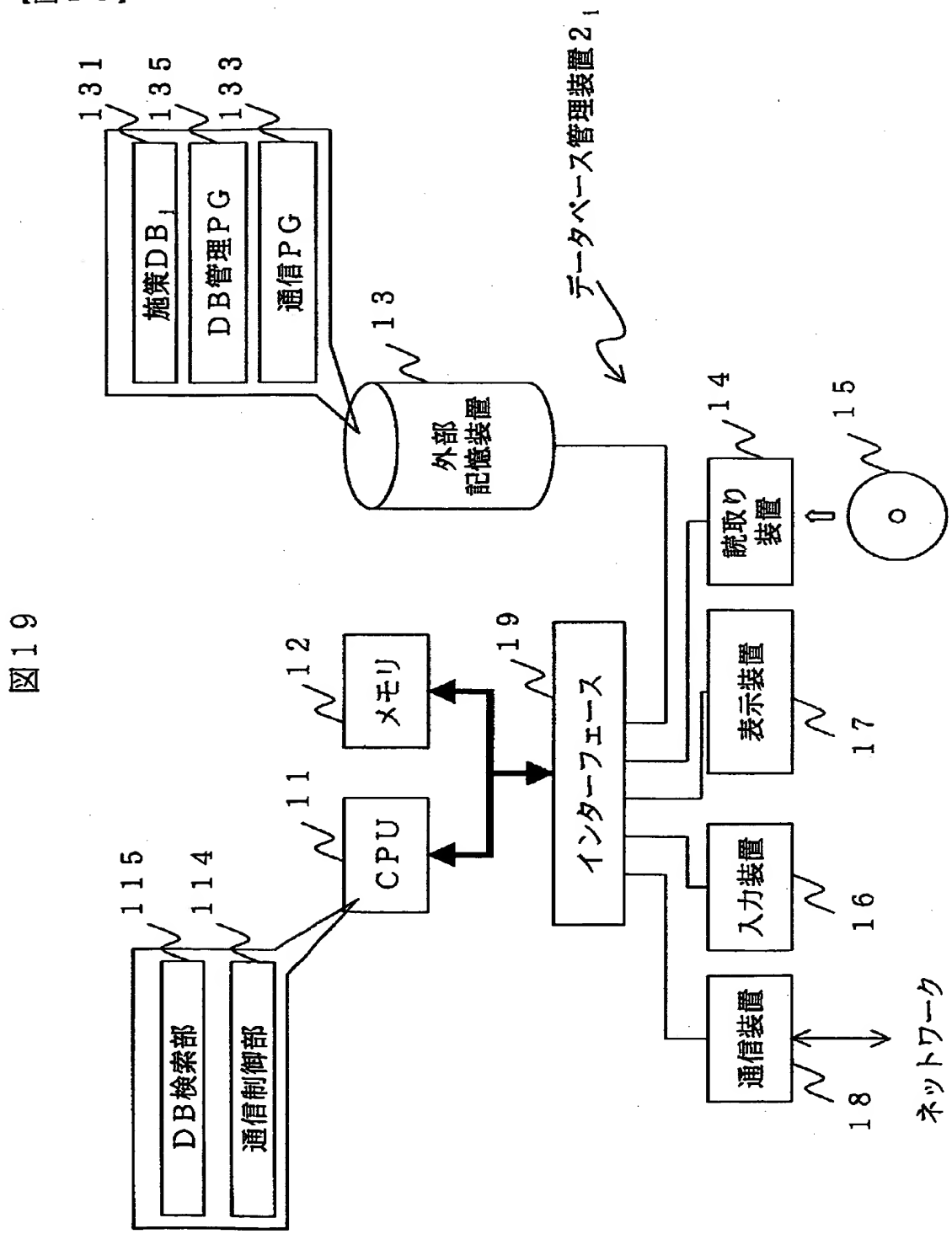
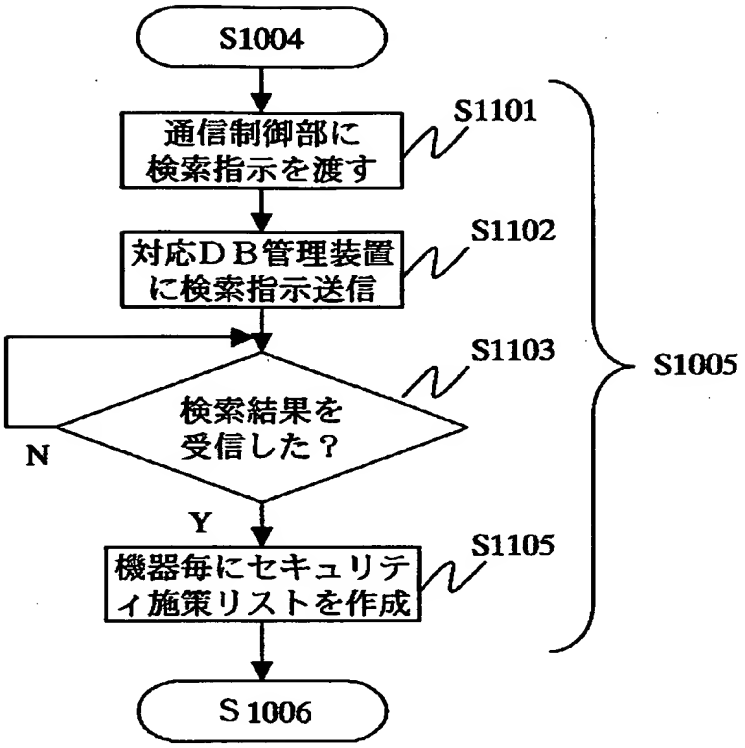

データベース管理装置２１
１３１
１３５
１３３
施策DB1
DB管理PG
通信PG
１３
外部記憶装置
１４
読取り装置
１５
１２
メモリ
１９
インターフェース
１１
CPU
表示装置
１７
１１５
１１４
DB検索部
通信制御部
入力装置
１６
通信装置
１８
ネットワーク

図１９

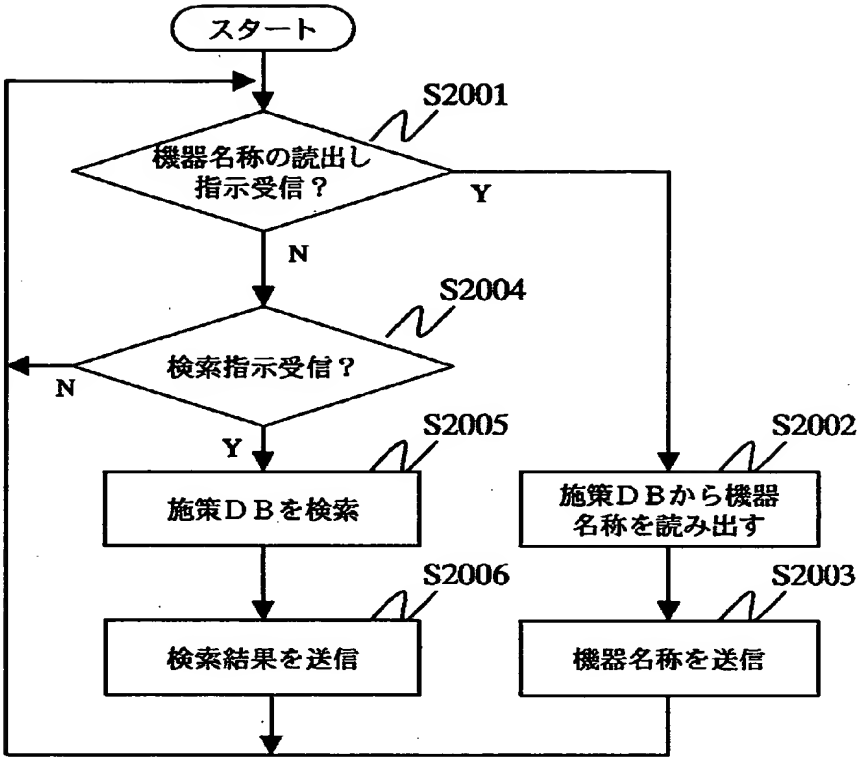
【図２０】

図２０


S1004
通信制御部に検索指示を渡す
S1101
対応ＤＢ管理装置に検索指示送信
S1102
検索結果を受信した？
S1103
N
Y
機器毎にセキュリティ施策リストを作成
S1105
S1005
S1006

【図２１】

図２１


スタート
S2001
機器名称の読出し
指示受信？
Y
N
S2004
検索指示受信？
N
Y
S2005
施策ＤＢを検索
S2002
施策ＤＢから機器
名称を読み出す
S2006
検索結果を送信
S2003
機器名称を送信

【書類名】要約書

【要約】

【課題】高度な専門的知識がなくても、システムのセキュリティ状態を評価したり、セキュリティ施策の作成を支援することを可能にする。

【解決手段】入力装置１６を介して、操作者より評価対象システムと当該システムを構成する各機器の指定を受け付ける。次に、外部記憶装置１３に格納されたセキュリティ施策データベース１３１を検索し、指定された評価対象システムの各機器に施すべきセキュリティ施策を読み出す。次に、指定された評価対象システムの機器毎に読み出したセキュリティ施策を対応付け表示装置１７に表示し、入力装置１６を介して、操作者よりセキュリティ施策の実施の有無を受け付ける。それから、受け付けた各機器のセキュリティ施策の実施の有無に基づいて、セキュリティ状態の評価を行ない、その結果を表示装置１７に表示する。

【選択図】図１

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所